(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 January 2002 (31.01.2002)

PCT

(10) International Publication Number
WO 02/08974 A2

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/GB01/03298

(22) International Filing Date: 23 July 2001 (23.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

0018047.1	21 July 2000 (21.07.2000)	GB
0111978.3	16 May 2001 (16.05.2001)	GB

(71) Applicant *(for all designated States except US)*: **NEXXGEN LIMITED** [GB/GB]; Albany House, Market Steet, Maidenhead SL6 8BE (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **WREN-HILTON, Giles, Martin** [GB/GB]; Field View, coldmoorholm Lane, Bourne end, Buckinghamshire SL8 5PS (GB).

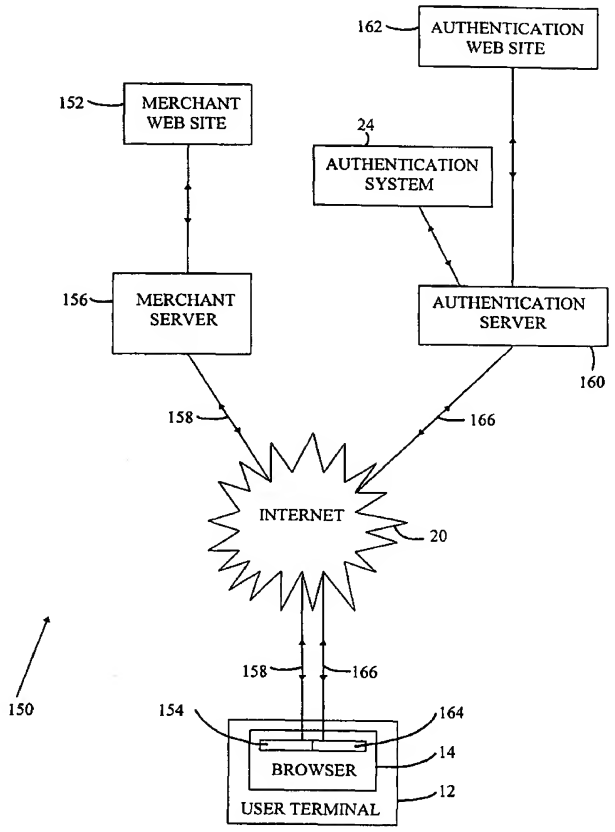
(74) Agents: **AHMAD, Sheikh, Shakeel** et al.; David Keltie Associates, 12 New Fetter Lane, London EC4A 1AG (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF,

[Continued on next page]

(54) Title: IMPROVEMENTS RELATING TO THE SECURITY OF AUTHENTICATION SYSTEMS



(57) Abstract: A method of and system for authenticating a personal authentication store such as a prepayment card for use in authentication the identity of a user is described. The method comprises generating a challenge by: receiving a unique identifier of the personal authentication store; identifying first and second subsets of predetermined data elements using the unique identifier; selecting a data element from the first subset and transmitting the data element to the user as an authentication challenge. Each subset has been previously selected from a corresponding larger set of the data elements and each data element of the first subset corresponds to a specific one of the data elements of the second subset. The authentication is determined by receiving a response to the authentication challenge from the user that has been determined by use of information provided on the personal authorisation store; and issuing an authentication signal if the response comprises the specific data element of the second subset that corresponds to the data element of the first subset used for the challenge.

WO 02/08974 A2

CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

IMPROVEMENTS RELATING TO THE SECURITY OF AUTHENTICATION SYSTEMS

The present invention concerns improvements relating to the security of authentication systems and provides, more specifically, though not exclusively, a method of and an apparatus for simple, low cost personal authentication over non-secure communications channels such as the Internet or a public telephone network.

Whilst the sophistication of our communications systems has rapidly evolved in recent years, such that we can now readily communicate with each other or with machines around the world, so too has the fraud that is committed via these systems. Nevertheless, given that system architectures control access throughout a system by employing user identities, most fraud still requires the impersonation, in some form, of another individual. Accordingly, system users are usually required not only to identify themselves, but also to provide some other means by which the system can validate them as an authentic user.

All known methods of authentication rely on one or more of the following factors being provided in additional to a user's declared identity, namely (1) something that the user knows, (2) something that the user has or (3) something that the user is. The reliability of a method increases with the number of authentication factors that it combines. System facilities are not made available to a user until their identity has been authenticated, namely by checking that the additional information provided matches that stored centrally on a system database.

An example of the type of information which a person might know, but others will not generally know about them, is their mother's maiden name. Typically, this information is provided to a system when registering as a new user. It is chosen as a system variable because it is easy for the user to remember. Unfortunately, it is also readily discoverable by unscrupulous individuals.

A more robust example of known information is a memorised password - commonly used for authenticating computer users or users of Internet-based services. This will usually be set, in the first instance, by a system administrator and then communicated to the individual who has been registered to use the system. When the set password is first used, the user will usually be given the opportunity to re-set it to something which they can readily recall.

Certain limitations may be enforced on the choice of a new password, for example a system may require passwords to contain non-alphanumeric characters. Constraints on what characters may be used are intended to make the system more resilient against so-called 'dictionary attacks' made by computer hackers. Many users base their passwords on real words and so hackers attempt to gain access to systems by creating algorithms which systematically work through a database, or 'dictionary', of common words or phrases. The introduction of non-alphanumeric characters increases the number of possible password variants, but this only makes passwords more time-consuming to crack and hackers have responded by adapting their algorithms to substitute in random non-alphanumeric characters as required and to process the variants at an ever-increasing rate.

The number of password-protected systems used by individuals in the course of their day-to-day lives is steadily increasing. To avoid having to carry around a large bunch of virtual keys, people tend to employ the same or similar passwords for accessing different systems. Unfortunately the consequence of this is that if one password becomes known, it can be relatively straightforward to deduce the others belonging to the same individual. Alternatively, there is a temptation to keep a list of one's passwords rather than relying on committing them to memory, which of course further compromises their security.

Passwords which are comprised exclusively of numbers are referred to as personal identification numbers, or PINs, and similar limitations to those outlined above apply.

The second factor mentioned above which is used for authentication purposes, namely something that the user has, relies on the user producing an item which verifies that they are who they have declared themselves to be. Whilst this removes the burden of having to memorise information from individuals, they must instead remember to carry the relevant authentication item on their possession.

Examples of items that a person may be asked to produce include a driving licence, a passport or an identity card. However, all of these items must be assessed by another person whereas today our interaction is increasingly with machines. Accordingly, a separate record of our identity can be stored on a personal portable device which can be read by machines. For example, a so-called *smart card* is a plastic card of the same dimensions as a credit card but with limited processing and data storage capabilities. However, machine-readable identity cards require expensive equipment to be installed at all points where authentication is required and so the coverage offered by this solution is limited.

When the sites where authentication is required are restricted to computer terminals, for accessing computer or Internet based services, it is possible to use small handheld electronic devices, known as *tokens*, as a means of providing authentication. The token generates statistically random numbers by executing an algorithm which generates pseudo random numbers. A copy of the token's algorithm is stored centrally by the computer system, so that the user is authenticated if the number generated by the token matches that generated by the stored algorithm. Tokens may be independent devices featuring a liquid crystal display, a key pad and an on-board power source, whereby the user enters a challenge received from the central computer system into the token and is provided with the response they should give. Alternatively, tokens can be devices which are connected to a computer system to generate and communicate authentication data directly; these devices are commonly referred to as 'dongles' but again they require specialist readers to be installed.

Tokens contain delicate electronics, though, which must be protected from physical extremes such as temperature, humidity, vibration and shock. Special casing is required which, in addition to the cost of the electronic components, makes the tokens expensive to manufacture. Certain physical environments preclude the use of tokens as a means for authentication - for example if there are strong magnetic fields. The cost of tokens, presently around the $80 mark, dictates that they are only issued to those employees whose jobs are deemed to require such security; this clearly does not meet the requirements of a global or mobile workforce. In addition to the above, if a person is issued with multiple tokens to access a number of different systems, then the physical size of the tokens will become a cumbersome inconvenience.

The problems associated with memorising information or carrying authentication devices around on one's person do not apply to the third factor for authentication, that is using a non-varying personal characteristic of the individual. So-called *biometric* methods of authentication, where the input to an authentication system could be a fingerprint, a voice sample or a retinal scan, say, have captured the popular imagination, but again require expensive special-purpose equipment which makes the widespread use of this type of authentication presently implausible. In addition, there are also privacy issues associated with the storage and use of biometric data.

Of course there is a need for all of the parties involved in a communication to authenticate each other. For example, payment cardholders have been the victims of fake automatic teller machines which have been stationed in high streets to record financial account details and PIN numbers. Similarly, bogus Web sites exist purely to elicit payment card details.

Across the Internet, the use of the SSL (Secure Sockets Layer) protocol by Web browsers provides a partial solution, albeit complex for the layman to understand and use effectively. Web browsers insert a yellow padlock on the browser bar if a Web site is deemed to be authentic and a secure channel for communication has been established. However, this technology is based on public key infrastructure which

relies on a hierarchy of trust. Ratification of the hierarchy is complex and difficult to achieve.

It is desired to overcome or substantially reduce some of the abovementioned problems. More specifically, it is desired to provide an authentication method and apparatus which is easy to use, has general applicability, is economic to implement and provides a measure of authentication for all of the parties involved in a communication.

The present invention resides in the appreciation that the degree of security required for most personal authentication solutions need not be absolute and that, as a result, an authentication system can be provided, which is relatively secure yet easy-to-use and significantly low-cost, based on a challenge/response mechanism where the response is a readily selectable option provided on a portable personal authentication store.

More specifically, according to one aspect of the present invention there is provided a personal authentication store, for use in authenticating the identity of a user by determining a response to an authorisation challenge, the authentication store comprising: a unique identifier for identifying the authentication store and hence the identity of the user; a first subset of a plurality of humanly readable elements; and a second subset of a plurality of humanly readable elements, each subset having been selected from a group of elements from a larger corresponding set and each element of the first subset being visually related to a specific one of the plurality of elements in the second subset, wherein the unique identifier is related to each element of the first subset and to each respective corresponding visually related element of the second subset by machine stored information external to the store such that authentication of the personal store requires the use of the machine stored information to verify the visual relationship between an element of the first subset provided as the authentication challenge and an element of the second subset provided as the response thereto.

The provision of the correct response to an authentication challenge on a portable personal authentication store makes the operation of the authentication system very simple in that the user does not have to remember any password but rather simply selects a matching response to the challenge to authenticate themselves to the authentication system.

The personal authentication store does not have to be electronic and does not require any special electronic reading equipment thereby significantly reducing its cost but increasing its portability and its ease of operability.

It is to be appreciated that the term 'humanly readable element' is intended to cover any visual identifier such as an icon or a colour having a distinct name associated with it which is provided on the store in place of that written name. Also the term 'unique user identifier' can be a number, barcode or any representation of an alphanumeric number unique to the personal store. It can also be a serial number which is used in the production of the card and in its distribution. In addition, the term 'subset' or 'set' is intended to mean a group of data elements which share a common feature, such as a category or colour, the subset being a selection from a defined set. Furthermore, the term 'authenticating' is intended to mean a process of confirming electronically a claimed relationship or identity.

It is the above-mentioned visual relationship that is apparent to the user, which enables the user to identify, in a very simple manner, the correct response (element from the second subset) to the received challenge (element for the first set) such that the user can be authenticated. The visual relationship between the elements of the first and second subsets can be achieved in many ways. For example, it may comprise a positional relationship, such that by virtue of how the elements of the first and second subsets are positioned, there is only one member of the second subset that corresponds to the challenge member of the first set.

Also the relationship can be a colour relationship or a graphical relationship such that appearance of the personal data store can be enhanced to make the store more customisable in appearance. This can make the store, such as a card, far more attractive to younger users, for example.

The elements of one of the first or the second subsets may comprise the features of the visual relationship. This advantageously minimises the amount of space required on the portable data store for displaying each challenge and associated response. This is because the elements of the first or second subsets can be made up of different colours and the colours themselves can be the responses or the challenges. Also, it is possible for one subset of elements to be displayed and the positional relationship with parts of the store (e.g. top left-hand corner) can be used to identify the required response.

Preferably, the elements of the first and second subsets comprise alphanumeric characters. The advantage of these types of characters is that they are readily transmittable across data networks such as the Internet or over the public telephone network (where input from the authentication card holder of non-numeric data would be more challenging than entering numeric data using the telephone's keypad). Also the invention is particularly easy to use for people of all ages and requires little to no training on the part of the user.

The alphanumeric characters preferably have a minimum font size of ten points. If the font size is any smaller than this then the characters become too difficult for the average user to read correctly and would decrease the simplicity and ease of use of the personal store.

Preferably one of the first and second subsets comprises words and the subset of words comprise words selected from a list of words suitable to minimise confusion when verbally spoken across a telephone network. This again makes the challenge/response less prone to errors when used in an aural authentication check. More preferably, the

subset of words comprise nouns. This type of element is relatively simple to recognise and use, which further prevents errors.

Preferably the words in the first subset are arranged in alphabetical order to facilitate the user rapidly finding the word from the presented subset on the store and reading back the corresponding response number into a terminal connected to an authentication system. Furthermore, the possibility of an error can be reduced by having a different type of information in the first subset to that provided in the second subset. More preferably, the information in the first and second subsets is non-personal to users such that even if this data is obtained unscrupulously, it would not compromise the user.

There are a number of factors governing the size of each subset provided on the authentication store. One is the number of elements that can be displayed on the store along with whatever other information is displayed on the store such that someone of average eyesight can easily read them without straining their eyes. Another is that the larger the size of each subset, the less chance there is of someone successfully intercepting an unencrypted communication channel carrying the card serial number, or information from the selected elements of the subsets will be able to fraudulently use the information so acquired. To a lesser extent, the smaller the number of information sets, the greater the degree of assurance that the authentication store holder has that he is dealing with a valid authentication system by minimising the chance of an impostor authentication system correctly guessing information from any subset on the authentication store.

For further security, the information in the first or second subsets may be rendered on the authentication store in a colour other than black or white. This may help prevent casual (black and white) photocopying of the card.

To further prevent casual photocopying of the authentication store, many well-known anti-copy techniques may be used, such as preparing the information-bearing surface of the authentication store with an ink, coating, varnish or film whose properties include the reflection and/or diffraction of the light source in a photocopier, which prevents casual

photocopying. Another method to achieve this is to render the authentication store in such a way that the some or all of the information is not visible from straight in front of the card by, for example, using a lenticular covering.

Preferably the personal authentication store is provided as a simple plastics card. The first and second subsets may be rendered on one face of the card having width and height dimensions substantially in accordance with standard ISO 7810, or on one face of a card which when folded has similar width and height dimensions. The advantage conferred by this feature is that it may be conveniently carried on the person in a wallet or purse or similar container designed for ISO 7810 cards. It is a further advantage for the card to be much thinner than ISO 7810 financial transactions cards (e.g. credit cards) so that the authentication card may be placed with other cards while adding a minimum of extra thickness to the cardholder's wallet or purse. Thinner cards use less of the material used for card manufacture (such as PVC or polyester), which is beneficial to the environment and reduces manufacturing costs.

In one embodiment, the authentication store is packaged in such a way as to ensure that no-one other than the intended user of the card has sight of the first and second subsets prior to the intended user obtaining the card. This may be achieved by using well-known tamper-evident devices such as envelopes, or stores (cards) with removable perforated edges or stores with rub-removable ink or a scratch-off coating acting as a covering means all of which facilitate an irreversible process to render the information sets visible to the human eye.

The authentication store (card) and/or the packaging may feature a visible code, such as a serial number, the purpose of which is to uniquely identify the card at any point in the distribution process from the card manufacturer to the end user. This latter feature is particularly important if the authentication card has a prepayment value associated with it, so that authentication card may be enabled or disabled, as required, at any stage in the distribution process. It is also important for the card issuer to know who has received

which authentication card, and this is achieved most securely if the authentication card is delivered to the user in an envelope, preferably a tamper-evident envelope.

The unique identifier may be a code such as a serial number, the purpose of which is to allow the cardholder to uniquely identify the card they are holding, for example to a system administrator or to the associated authentication computer upon initial registration of that card, without revealing any other information from the card. This code, or serial number, may be the same as, or related to, a visible code which may be seen prior to the store being given to the end user.

A specific and important advantage of the authentication store described above is that the authentication card holder is provided a reasonably high degree of assurance that he is dealing with a valid authentication system, not a bogus authentication system. More specifically, the response from the authentication system when the unique identifier of the personal authentication store is submitted can be considered a challenge-response mechanism from the user's perspective.

Another advantage of the authentication store is that it can be extremely low cost to manufacture. Also, when embodied as a card, its use does not require any special purpose terminal equipment other than a telephone device or a computer terminal connected to the Internet or connected to a computer network.

Whilst not providing the cheapest solution, the authentication store may comprise an electronic device in which the first and second subsets can be held and displayed. Preferably, in this case, the electronic device comprises a mobile telephone, a personal digital assistant or other mobile computing device which are all common portable devices which can simply be programmed without substantial cost to display the information that would be displayed on a card for example in addition their primary use.

Although conceived of primarily for personal authentication, another aspect of the invention provides the ability to offer secure prepaid services. Accordingly, the

authentication store may has a prepayment value associated with it and means for identifying the prepayment value to the user.

One field that can benefit from the advantages conferred by the present invention is that relating to, or concerned with, financial transactions and the authentication of those transactions to reduce or prevent fraud. The invention may be used in conjunction with a financial transaction card (e.g. a credit or debit card) to authenticate financial transactions and hence reduce the possibility of fraud. Alternatively, the authentication store and credit card information can conveniently be provided in one card, for example, on opposed faces, though this is not as secure as providing the financial and security information on separate cards. The personal authentication store together with an authentication system can be used for Cardholder Not Present (CNP) transactions over the Internet and over the telephone.

Another aspect of the present invention is an authentication method for use with the authentication card. An authentication system for implementing the method may take different forms according to the application for which the authentication is required and is here described in general terms. Usually, but not necessarily, the authentication system will form part of a larger computer system providing other services.

More specifically according to another aspect of the present invention there is provided a method of authenticating a personal authentication store for use in authenticating the identity of a user, the method comprising: receiving a unique identifier of the personal authentication store; identifying first and second subsets of predetermined data elements using the unique identifier, each subset having been previously selected from a corresponding larger set of the data elements and each data element of the first subset corresponding to a specific one of the data elements of the second subset; selecting a data element from the first subset and transmitting the data element to the user as an authentication challenge; receiving a response to the authentication challenge from the user that has been determined by use of information provided on the personal authorisation store; and issuing an authentication signal if the response comprises the

specific data element of the second subset that corresponds to the data element of the first subset used for the challenge.

Advantageously, the receiving step may comprise receiving a response to the authentication challenge from the user that has been determined by use of information provided on the personal authorisation store authentication described above.

The transmitting and receiving steps may comprise transmitting and receiving information over a telecommunications link such that remote authorisation of a user can be carried out. This is clearly advantageous as it enables CNP transactions to be authorised. Preferably, the transmitting and receiving steps are carried out via the Internet or via a short messaging service (SMS) exchange for mobile communications.

The selection step may comprise selecting an element of the first data subset at random. This increases the difficulty for unscrupulous people detecting a sequence of challenges and responses such that they can predict what the next challenge will be. However, the selection step may also comprise selecting an element of the first data subset randomly on first use of the personal authentication store and thereafter selecting an element of the first data subset deterministically such that a previously selected element has a lower chance of being selected than a previously not selected element. This balances the use of all the different elements in the first data set again to prevent someone working out what a response to a given challenge should be.

Alternatively, the selection step may comprise selecting an element of the first data subset sequentially in the order that the elements are displayed on the user's personal authentication store. Whilst this is not as secure a technique in some respects, it does have the benefit that the user is aware of what is the next challenge that they should be asked and so they are able to detect fraud by a challenge being asked out of the sequence presented on their card.

The method may further comprise making prepaid services available to the user in response to issuance of the authentication signal. This would typically comprise reducing a prepayment value stored in a prepayment field in accordance with the use of the prepaid services. The application of the authentication method to prepaid services provides an additional layer of security to existing prepayment systems.

The method may further comprising processing a payment transaction in response to the issuance of the authentication signal, such that on-line Internet shopping can be carried out rapidly and effectively.

According to another aspect of the present invention there is provided a system for authenticating a personal authentication store for use in authenticating the identity of a user, the system comprising: a receiving means for receiving a unique identifier of the personal authentication store; identifying means for identifying first and second subsets of predetermined data elements using the unique identifier, each subset having been previously selected from a corresponding larger set of the data elements and each data element of the first subset corresponding to a specific one of the data elements of the second subset; selecting means for selecting a data element from the first subset; transmitting means for transmitting the data element to the user as an authentication challenge; the receiving means being arranged to receive a response to the authentication challenge from the user that has been determined by use of information provided on the personal authorisation store; and issuing means for issuing an authentication signal if the response comprises the specific data element of the second subset that corresponds to the data element of the first subset used for the challenge.

The authentication system is set up to accept an input that uniquely identifies which authorisation store, is to be authenticated. Normally this would be a serial number associated with the card, and may arrive at the authentication system indirectly, for example by a related system which has received other information identifying the user. The authentication system has available to it a database of records, including the record showing the first and second subsets of elements which are uniquely related to each

other, that corresponds to the unique identifier or a means of recreating the first and second subsets associated with the unique identifier. The authentication system randomly or deterministically selects one of the elements of the first subset as a challenge to the user. This challenge is submitted to the user and the user looks at the first and second subsets of elements on the authentication store and finds the response information corresponding to the challenge. The user then submits to the authentication system this response information, or information derived therefrom. The authentication system takes this response and if the response corresponds to the element of information in the second subset corresponding to the element selected for the challenge, the authentication system generates a positive authorisation signal; otherwise the authentication system generates a negative authorisation signal.

The authentication system may feature as a method of input, from a user to the system they are using, an on-screen representation of a keypad which the user uses with an onscreen pointer (such as that controlled by a mouse, trackball or similar device) and mouse button (or similar button) to enter the user's response to the authentication system's challenge. The advantage of this method is that by avoiding using the computer's keyboard, there is less chance that the user's response can be captured by a covert keyboard-monitoring device or program.

The authentication system may feature a method of encrypting the user's response whereby the authentication system submits a random data challenge along with the information challenge. The user's response is used as a symmetric encryption key to encrypt the random data challenge, which is then sent back (via a web server) to the authentication system. The authentication system decrypts the returned encrypted random data challenge with the associated information from the challenge and if the results match (that is, if when decrypted by the associated information from the challenge the same random data is generated as that random data sent in the random data challenge), the system generates an authorisation signal. The advantage of this method is that the user's response is not sent back, and cannot therefore be captured by a covert communication channel listening device or program.

The sequence of steps which define the present aspect of the invention, along with the degrees of randomness protection afforded by using, for example, four to six digit response numbers, means that it is difficult for a genuine cardholder to later deny that he authorised a given transaction. This feature reduces the likelihood of transaction repudiation.

The present invention may be used in conjunction with other well-known security, cryptographic and authentication techniques and systems to further enhance many aspects of the overall security of a given system. One example of an additional mechanism that may be used to provide further security to the invention is the use of encryption systems such as SSL on the Internet to encrypt the data flow between the computer being used by the cardholder and the web server they are connected to.

There are further security advantages conferred by using this authentication card and system in conjunction with memorised information such as a password or PIN. When used in combination with memorised information, the enhanced system is a two-factor authentication system.

The present invention may be used in any field where a low-cost authentication mechanism is of benefit. Although not described in detail above, the authentication store and authentication system may also be used to provide authentication services over a voice communications channel such as that provided by a telephone. The challenges from the authentication system may be spoken to the cardholder and the response from the cardholder spoken back to a speech recognition unit and passed to the authentication system or the cardholder may respond using the keys on the cardholder's telephone keypad.

The present invention also relates to a method of configuring a personal authentication store, for use in authenticating the identity of a user by determining a response to an authorisation challenge, the method comprising: determining a unique identifier for identifying the authentication store; selecting a first subset of a plurality of humanly readable elements from a corresponding larger set of the elements; selecting a second

subset of a plurality of humanly readable elements from a corresponding larger set of the elements; relating the unique identifier to the first and second selected subsets and relating elements within the first subset to corresponding elements within the second subset, such that the elements of the first and second subsets can be used to validate the authenticity of the personal authentication store; and storing the unique identifier, the first subset and the second subset in the personal identification store, such that each element of the first subset is visually related to a specific one of the plurality of elements in the second subset, thereby enabling the user to determine which element of the second subset is to form a response to a challenge comprising an element of the first subset.

Either of the selecting steps may comprise selecting the plurality of humanly readable elements which make up the first or second subsets randomly from the corresponding larger set of elements. This provides a good way of preventing fraudulent mass manufacture of authentication cards.

Also, either of the selecting steps may comprise selecting the plurality of humanly readable elements which make up the first or second subsets deterministically such that there is no duplication of elements in any of the subsets. This is beneficial in that it avoids confusion in the generation of a response and also reduces the chances of a guessed response being correct.

In one preferred embodiment of the authentication store, the word or words used in the first subset are chosen from a dictionary of suitable words. The suitability of words is governed by many factors including but not limited to the type of word (nouns are better than adverbs), the number of letters (preferably no more than eight has been established by the inventor), the number of syllables (no more than two) and how common usage of the word is – common words being more easily recognised, particularly over the telephone, than obscure ones – and the reading age (preferably no higher than eight) associated with a given word. In preparing words to go on a particular card for example, a further check by the first and second set generating computer may be made to remove

and replace words that may be easily confused (by dyslexic misreading of the letters, similar phonetic sound, or otherwise).

If the second subset comprises numbers, these corresponding numbers may be of any length but four to six digits provides a good balance between ease-of-use and being randomly guessed. A four digit number has a one in ten thousand chance of being guessed correctly and a six digit number has a one in one million chance of being randomly guessed.

Accordingly, the elements of the first or second subsets may comprise alphanumeric characters and the storing step may comprise arranging the elements of the first or second subsets in alphabetic or numeric order in the personal authentication store. This advantageously provides a fast look up for the user.

According to another aspect of the present invention there is provided a system for configuring a personal authentication store, for use in authenticating the identity of a user by determining a response to an authorisation challenge, the system comprising: determining means for determining a unique identifier for identifying the authentication store; first selecting means for selecting a first subset of a plurality of humanly readable elements from a corresponding larger set of the elements; second selecting means for selecting a second subset of a plurality of humanly readable elements from a corresponding larger set of the elements; relating means arranged to relate the unique identifier to the first and second selected subsets and relating elements within the first subset to corresponding elements within the second subset, such that the elements of the first and second subsets can be used to validate the authenticity of the personal authentication store; and storing means arranged to store the unique identifier, the first subset and the second subset in the personal identification store, such that each element of the first subset is visually related to a specific one of the plurality of elements in the second subset, thereby enabling the user to determine which element of the second subset is to form a response to a challenge comprising an element of the first subset.

Brief Description of the Drawings

Methods and apparatus according to presently preferred embodiments of the invention for authenticating individuals over non-secure communications channels will now be described by way of example, with reference to the accompanying drawings in which:

Figure 1 is a schematic block diagram showing a security system for authenticating users who wish to access a secure corporate Web site, according to a first embodiment of the invention;

Figure 2 is a plan view of an authentication card which is used in conjunction with the security system of Figure 1, according to presently described embodiments of the invention;

Figure 3 is a schematic block diagram showing an authentication system as featured in the security system of Figure 1, according to presently described embodiments of the invention;

Figure 4 is a table containing data which identifies users to the authentication system of Figure 3, according to presently described embodiments of the invention;

Figure 5 is a table containing data which is also stored on the authentication card of Figure 2, according to presently described embodiments of the invention;

Figure 6 is a flow diagram showing the steps involved in authenticating a user, according to the first embodiment of the invention;

Figure 7 is a flow diagram showing the steps involved in generating a challenge that is submitted to the user as a step in Figure 6;

Figure 8 is a schematic block diagram showing a security system for authenticating users via a centralised authentication authority, according to a second embodiment of the invention;

Figure 9 is a flow diagram showing the steps involved in authenticating a user, according to the second embodiment of the invention;

Figure 10 is a plan view of an alternative authentication card from that shown in Figure 2, according to presently described embodiments of the invention;

Figure 11a is a plan view of the reverse side of the authentication card shown in Figure 2 when it features a set of payment card details, according to presently described embodiments of the invention;

Figure 11b is a plan view of a tamper-evident envelope which can be used to package authentication cards, according to presently described embodiments of the invention;

Figure 12 is a plan view of a personal digital assistant which displays the authentication data provided on the authentication card of Figure 2, according to presently described embodiments of the invention;

Figure 13 is a schematic block diagram showing a system for generating authentication cards, according to the first and second embodiments of the invention; and

Figure 14 is a flow diagram showing the steps involved in producing a batch load of authentication cards, according to the first and second embodiments of the invention.

Detailed Description of Preferred Embodiments of the Present Invention

With reference to Figure 1, a security system 10 for implementing a first presently preferred embodiment of the invention is now described. The security system 10

determines whether a user terminal 12, featuring a Web browser 14, is granted access to a corporate Web site 16. The Web site 16 is hosted by a corporate server 18, which is accessible to the user terminal 12 via the Internet 20. A communications link 21 connects the user's Web site browser 14 to the corporate server 18. All communication with the corporate Web site 16 is controlled by the corporate server 18 liasing with the login engine 22 and the authentication system 24.

As mobile working practices increase, there is a growing need for corporate bodies to make their systems accessible via the Internet 20 rather than on corporate intranets whose network coverage can be extremely restrictive. However, the security of sensitive corporate information is paramount and so reliable authentication methods must be employed. Generally, at least two factors of authentication are required in order to gain access to sensitive information on a corporate Web site 16.

Accordingly, the corporate server 18 shown in Figure 1 is provided with a login engine 22, for checking whether a username and password supplied from the user terminal 12 are recognised, together with an authentication system 24 for determining a second factor of authentication. In performing the first of these authentication checks, the login engine 22 refers to a database 26 of user details. As a consequence of this, control of all communications with the Web site 16 is achieved by the corporate server 18

Figure 2 shows an authentication card 30 which is used in conjunction with the security system 10. The authentication card 30 is a personal item that is issued to all users of the corporate Web site 16. It stores information which is also held by the authentication system 24, such that the authentication system 24 can issue a user with a challenge and the user can refer to their authentication card 30 to provide an appropriate response. In what follows, the features of the authentication card 30 will be described in detail, as will further aspects of the security system 10, before an explanation is given of how the two are used in combination to validate a user.

The authentication card 30 has substantially the same dimensions as a standard credit card and is similarly manufactured from durable plastic. Embossed, or printed, on one face of the card are two sets of data, 32 and 34, each set containing a different type of data. Both of the data sets 32 and 34 each have twenty members. The first data set 32 appearing on the authentication card 30 is comprised of words 36 which are between three and seven characters long, whilst the second data set 34 consists exclusively of four digit numbers 38. Each data set member is unique within its data set.

The 'word' and 'number' data sets, 32 and 34 respectively, are arranged in separate columns on the authentication card 30, the columns being adjacent to oneanother such that there is a unique visual, positional correspondence between a word 36 and a number 38 appearing on the same row. The words 36 are ordered alphabetically to enable fast look up. Each data set column is split into two halves - the first ten members of each of the 'word' and 'number' data sets 32, 34 being presented on the left hand side of the authentication card 30 and the last ten members on the right hand side. As can be seen from Figure 2, this effectively gives rise to four demi-columns of data.

The authentication card 30 is also provided with a serial number 40, which uniquely identifies the card to the security system 10. This number is of assistance, for example, when the authentication cards 30 are manufactured. The serial number 40 is also stored as a bar code 42 on the authentication card 30, so that it may be read quickly when the card is passed through a bar code reader (not shown).

In order to prevent the authentication card 30 from being casually photocopied, the card is provided with a diffusion coating 43 as shown in the enlarged view of the card surface 44. Illuminating light from a photocopier is diffused by the coating 43, resulting in a copy of poor quality which prevents the 'word' and 'number' data sets, 32 and 34 respectively, from being deduced.

As mentioned above, information which is presented on a user's authentication card 30 is also stored by the authentication system 24 of the security system 10. The authentication system 24, which is suitable for use in all of the embodiments described herein, is shown in more detail in Figure 3. The authentication system 24 is comprised of a database 50, an authentication engine 52 and a random number generator 54.

The 'word' and 'number' data sets, 32 and 34 respectively, associated with a particular authentication card 30 are stored in authentication data tables (described in detail later) which are held in the database 50, there being one table per card. Each authentication data table is referenced by the serial number 40 associated with the corresponding authentication card 30. The authentication engine 52 uses the data stored for a particular authentication card 30 to generate a user challenge and to assess the user's response. The authentication system 24 is told which serial number 40 to process by the login engine 22 which refers to the database of user details 26.

Figure 4 shows a limited excerpt from a table of user details 60 which is stored in database 26, the table name being USER_DETAILS. Each row of the USER_DETAILS table 60 corresponds to a particular user of the Web site 16. The table is comprised of four columns, namely USER_NAME 62, PASSWORD 64, SERIAL_NO 66 and VALIDITY 68, such that the serial number 40 associated with a particular user's authentication card is stored alongside their username and password. It can be seen that the authentication card 30 shown in Figure 2 is assigned to the user with username 'N1ZAW'. The variable stored under the VALIDITY column 68 is provided so that the security system 10 can enable or disable the authentication of a particular authentication card 30 at any point in time.

An example of an authentication data table 80, for the authentication card of Figure 2, is shown in Figure 4. The authentication data table 80 is named after the serial number 40, namely 4072 3811 0987 2104, of the authentication card 30. The table is comprised of three columns, namely ROW_NUM 82, WORD 84 and NUMBER 86. Members of the 'word' data set 32 appear under the WORD column 84, whilst those

of the 'number' data set 34 appear under the NUMBER column 86. The variables under the ROW_NUM column 82 indicate the row number within the authentication data table 80. The authentication data is stored in the same row order as it appears on the authentication card 30, so that, for example, the word KITE and the number 6231 appear alongside ROW_NUM 10, whilst the word MOUSE and the number 2012 appear alongside ROW_NUM 11.

An authentication process 100, which is performed by the security system 10 of Figure 1 and requires the use of an authentication card 30, will now be described with reference to Figure 6. The authentication process 100 is a two-factor authentication process, the first factor relying on standard username and password validation, the second factor comprising validation of a response from a user to a specific issued challenge. If the response given by the user is judged to be correct, access to the Web site is made available to the user.

The authentication process 100 begins when a user gives the URL address of the corporate Web site 16 to their browser 14. At step 102 of the authentication process 100 the corporate server 18 presents the user with a standard login screen, prompting them to enter their username and password.

When the user's login details are received by the corporate server 18 at step 104, they are submitted for verification to the login engine 22 which checks if they are stored in the USER_DETAILS table 60 of Figure 4. If the login details are not recognised, for example if the username supplied is not found under the USER_NAME column 62 or if the password supplied with a recognised username does not match the corresponding password stored under the PASSWORD column 64, then at step 106 in the authentication process 100 the corporate server 18 generates and sends a message to the user's browser 14 stating the same. In such a circumstance, the user may be permitted a limited number of attempts to log in correctly.

Alternatively, if the login engine 22 finds the supplied username and password to be valid according to the USER_DETAILS table 60, then the authentication system 10 validates the user according to its first factor of authentication. Accordingly, at step 108 in authentication process 100, the login engine 22 retrieves the serial number 40 from the table USER_DETAILS 60 that is associated with the supplied username and forwards it to the corporate server 18.

The serial number 40 identifies the authentication data table 80, shown in Figure 5, which holds a record of the data issued on the user's authentication card 30. The corporate server 18 sends the serial number to the authentication system 24, which uses it to generate a challenge to be issued to the user as part of the second factor of authentication. At step 110 in the authentication process 100, the authentication system 24 uses the serial number to select a word and a corresponding number from the user's authentication data table 80. The selected word is used to form the user challenge, whilst the selected number is stored as an expected response. This step is described later in greater detail with reference to Figure 7.

The corporate server 18 issues the challenge to the user, via the communications link 21, at step 112, such that a pop-up window (not shown) containing the selected word appears at the user's browser 14. The pop-up window explains that the Web site which the user has addressed is a secure Web site and that the user must be authenticated before access will be granted. It instructs the user to refer to their authentication card 30, locate the selected word displayed in the pop-up window on the card and then enter the number associated with the word as a response to the challenge.

The user's response is received by the corporate server 18 at step 114 in the authentication process 100 and is subsequently transferred to the authentication system 24. At step 116 the authentication system 24 makes a comparison between the expected response, which was stored at step 110, and the received response. If the number supplied by the user is identical to that of the expected response, then the user is judged to have satisfied the second factor of authentication and, accordingly, the

authentication system 24 generates an authentication signal at step 118. However, if the user's response does not match the expected response then the authentication system 24 generates a rejection signal at step 120.

These signals determine whether the user is granted access by the corporate server 18 to the Web site 16. When the corporate server receives an authentication signal, as at step 122 in the authentication process 100, it closes the pop-up window and connects the user's browser 14 to the Web site 16. Accordingly, the user is then able to access the sensitive corporate information which is held on the Web site 16 in accordance with that user's security privileges. If a rejection signal is received by the corporate server 18, it sends another message within the existing pop-up window to the user at step 124 informing them that their response was incorrect and that they have not been granted access to the Web site 16. In some user selected cases, the message can however ask the user if they would like to send a different response to the same challenge (although this option would only be available for a limited number of incorrect response iterations). It is preferred not to give a new challenge word to the user for security reasons.

The processing conducted by the authentication system 24 in generating a challenge for the user at step 110 of Figure 6 is now described in Figure 7. A challenge generation process 130 commences at step 132 when the authentication engine 52, shown in Figure 3, receives a serial number from the corporate server 18 identifying a particular authentication data table 80. At step 134 the authentication engine calls the random number generator 54, which randomly selects a number between 1 and 20 (as there are twenty possible challenge/response pairs in each authentication data table 80) using any of the well-known random number generation algorithms. The authentication engine 52 receives the randomly selected number at step 136.

Using these two pieces of information, namely the serial number and the random number, the authentication engine 52 accesses the appropriate authentication data table 80 from the database 50 and selects a word and a corresponding number from a

particular row. The authentication data table 80 is comprised of twenty rows of data and the authentication engine 52 selects the word and the number from the nth row, where n is the number obtained from the random number generator 54. The authentication engine 52 transmits the selected word to the corporate server 18 at step 140, whilst storing the corresponding number in a temporary variable for later use in the comparison with the received response at step 116 of the authentication process 100.

Randomly selecting a word and a corresponding number in this way, prevents the challenge that will be issued to the user from being known in advance, thereby improving the security of the authentication process 100.

The second presently preferred embodiment of the invention will now be described with reference to Figures 8 and 9. This embodiment demonstrates how the present invention may be implemented using a centralised authentication system, rather than an authentication system which is specific to one entity as described in the first embodiment. A centralised authentication system is particularly suited to the on-line shopping environment, which has proved to be an easy target for payment card fraud.

When ordering goods or services from a merchant Web site a user must also provide their payment card details so that the merchant can take payment under a Cardholder Not Present transaction. However, there is a problem if details of a valid payment card have been obtained fraudulently and the payment card has yet to be 'stopped'; the merchant is not alerted to the fraud and so allows the purchase to proceed. The second embodiment of the present invention overcomes this problem by introducing a further factor of authentication into the on-line ordering process. Prior to transmitting their payment card details, users are required to authenticate themselves with an authentication authority which independently informs the merchant of the authentication result. This additional information allows merchants to refuse to accept payment from non-authenticated individuals and discourages valid payment card details from being used with false identities.

Figure 8 shows a security system 150 for implementing the second embodiment. Here, a user accesses a merchant Web site 152 via a first instance 154 (browser window) of the user's Web browser 14. The merchant Web site 152 is hosted by a merchant server 156, which the first browser instance 154 connects to via the Internet 20 and a communications link 158. An authentication server 160 of a centralised authentication authority is also accessible via the Internet 20. The authentication server 160 is provided with an authentication system 24, as described in the first embodiment, and also hosts an authentication Web site 162. The user terminal 12 connects to the authentication server 160 via a second browser instance 164 (a pop-up browser window) using a communications link 166 (as is described in more detail later).

Users of the security system 150 are provided with authentication cards 30, as in the first embodiment of the present invention. Accordingly, a description of the authentication cards 30 will not be repeated here, although possible variations of the authentication cards will be described in due course. However, a key difference between the authentication cards 30 of the first and second embodiments is their scope of use. As the authentication cards 30 of the second embodiment are issued by a centralised authentication authority, they can be used to validate users to any entity, whereas the cards issued in the first embodiment are restricted to authenticating users to a specific corporation.

When a user wishes to purchase goods or services from a Web site 152, the above-described security system 150 carries out an authentication check. In general terms this involves the user being temporarily diverted from the merchant Web site 152 to the Web site 160 of a centralised authentication authority. The user is then issued with a challenge and responds according to the information held on their authentication card 30. The user's response is assessed by the authentication system 24 which determines whether the user is recognised. An appropriate message concerning the authenticity of the user is transmitted to the merchant Web site 152 and the user is duly returned there.

Processing on the merchant Web site 152 can then proceed according to the authentication result.

The way in which a user interacts with the security system 150, and how the security system 150 determines the authenticity of the user, will now be described in detail with reference to Figure 9. Figure 9 shows the steps involved in an authentication process 170. Whilst browsing the merchant Web site 152, the user comes across some goods or services that they wish to order. After indicating their order to the Web site 152, the user is presented, at step 172 of the authentication process 170, with a message in the first browser instance 154 inviting them to seek authentication via the centralised authentication authority. If the user accepts the invitation then, at step 174, the merchant server 156 instructs the user browser 14 to create the second instance 164 of itself. This communication is made via the existing communications link 156. The second browser instance 164 opens in the foreground of the display of the user terminal 12, whilst the first browser instance 154 (displaying the merchant Web site 152) is maintained in the background. In addition to this, the merchant server 156 instructs the second browser instance 164 to access the authentication Web site 162 by providing its URL. Accordingly, the second browser instance 164 establishes the communications link 166 with the authentication server 160.

At step 176 of the authentication process 170, the authentication server 160 sends a message to the second browser instance 164 asking the user to enter the serial number 40 of their authentication card 30, which the user duly does. After the serial number is received by the authentication server 160, steps 110 to 120 of the authentication process 100, shown in Figure 6, are executed as indicated by step 178. Accordingly, the user is challenged through the second browser instance 164 and provides a response which enables the authentication system 24 to generate either an authentication signal or a rejection signal. This signal is then transmitted from the authentication server 160 to the merchant server 156 at step 180. The authentication server 160 uses the existing communications links between itself and the merchant server 156, namely communications links 166 and 158, for this purpose. It then

instructs the second browser instance 164 to terminate the communications link 166, causing the second browser instance 164 to disappear from the user's display. The user is then returned to the merchant Web site 152 displayed by the first browser instance 154.

The merchant Web server 156 then informs the user of the authentication result received from the authentication server 160. If an authentication signal was received, the merchant Web site 152 prompts the user for their payment card details. Payment for the order is then transmitted and accepted in the usual way. Alternatively, if a rejection signal is received at step 180 then the merchant Web site 152 issues a message stating that the user's order has been refused.

It is to be appreciated that as an alternative to the above described embodiment of authentication of Web merchant transactions, the authentication can be acquirer driven rather than merchant driven. More specifically, the sequence of events would be that firstly the user finds goods they wish to purchase on the merchant's Web site 152. The user then enters the financial transaction card number at their terminal 12, such as their credit card number. On receipt of this information, the merchant's Web site 152 sends a message to the computer of the card's acquiring bank (not shown) requesting authorisation of a desired payment transaction. At this stage, the acquiring bank's computer sends a message to the card issuing bank's computer (not shown) requesting authorisation of the desired payment transaction. The card issuing bank looks at a database record (not shown) corresponding to the financial transaction charge to see if the user has elected to have CNP transactions authenticated by a centralised authenticating authority. If authentication is required, a request for authentication is passed from the issuing bank to the authentication authority (comprising the authentication Web site 162, the authentication server 160 and the authentication system 24) which then carries out the authentication as described in the second embodiment. The result (positive/negative) of the authentication is then passed back to the issuing bank who pass a message back to the acquiring bank specifying whether the transaction has been declined or accepted. The message is then passed back to the

merchant Web site 152 for acceptance or rejection of the payment transaction proposed by the user.

The advantage of the above described alternative method is that the merchant and the acquiring bank need make no changes to their existing transaction processing system, only the issuing bank does, and logically it is the issuing bank who should implement systems to enhance security for themselves and their customers.

As mentioned earlier, the form of the authentication cards need not be restricted to that shown in Figure 2. For example, one of the data sets presented on the card could be a set of colours which are used to distinguish the members of a second data set. This is illustrated in Figure 10 by the authentication card 190, where shading has been used to convey different colours as indicated by the shading key 192. Five blocks of colour 194 are provided on the authentication card 190, each block being presented with a different colour. Members of a second data set, which is comprised of five words 196, appear in the colour blocks 194. A single word 196 is positioned within each colour block 194, such that if the challenge issued to the user is a colour they can respond with the corresponding word and vice-versa. Only the colour names need be stored next to the words 196 in the corresponding authentication data table 80, this table again being identified by the card's serial number 40 which is displayed at the bottom of the authentication card 190.

Another possible variation of the authentication card 30 is shown in Figures 11a and 11b. In this variation, payment card details are applied to the reverse face of the card shown in Figure 2, producing a payment/authentication card 200 as shown in Figure 11a. The payment card details comprise a Primary Account Number (PAN) 202, a date 204 from which the card may be used, an expiry date 206 beyond which the card cannot be used and a payment cardholder name 208. This information is also contained in an electronic chip 210 which is mounted on the same surface of the card. The payment/authentication card 200 is suitable for use in either the first embodiment, for example as a store charge card, or in the second embodiment, for example as a credit card. In a variation of the above-described payment/authentication card 200, the PAN

may act as the serial number of the authentication card, such that there would be no need to provide a serial number 40 for the authentication card.

The payment/authentication card 200 may be provided to the payment cardholder in a tamper-evident envelope 220, as indicated in Figure 11b. This prevents anyone other than the intended user of the card from gaining sight of the 'word' and 'number' data sets, 32 and 34 respectively, which will be used to authenticate the user. The payment/authentication card 200 is totally obscured from view when inside the envelope 220, but the card's serial number 40, and its associated barcode 42, are reproduced on the outside of the envelope as shown. This allows the card 200 to be uniquely identified at any point in the distribution process, from the manufacturer to the end user. The envelope 220 also displays a warning 222 to the recipient of the card, stating that the card will not suitable for use if its packaging has been tampered with. In this event, the recipient should contact the authentication authority who issued the card, informing them of the card's serial number. The payment/authentication card 200 may then be disabled via the validity variable 68 (shown in Figure 4). A new card assigning different 'word' and 'number' data sets to the user will then be issued by the authentication authority.

Users may find it more convenient to store a virtual copy of their authentication card 30 on a portable electronic device such as a personal digital assistant (PDA), rather than carrying the actual authentication card 30 on their person. Figure 12 shows a PDA 230 displaying the same authentication details as those provided on the authentication card 30. The display uses the same format as that employed on the authentication card 30, namely four demi-columns of the 'word' and 'number' data sets 32 and 34, respectively. The card's serial number 40, which is used to identify the user's authentication data to the authentication system 24, is also provided at the bottom of the screen. Accordingly, authentication authorities may issue their users with both a 'hard' and 'soft' copy of their authentication details, supplying them with simple software which can be loaded onto a personal computing device of the user's choice

for displaying the authentication card data. Software may also be provided for automatically receiving the challenge and transmitting a user selected response.

Production of the authentication cards 30 of the first and second embodiments will now be described, with reference to Figures 13 and 14. Figure 13 shows an authentication card generation system 240 which is comprised of a selection engine 242, the authentication system 24 of the previously described embodiments and a printing manufacturer's system 244.

The selection engine 242 selects the information that is to appear on a particular authentication card 30 and subsequently informs the authentication system 24 of its selections. It also instructs the printing manufacturer's system 244 to produce cards bearing the selected authentication information. Both the authentication system 24 and the card manufacturer's printing system 244 are updated by the selection engine 242 on a regular basis, after details of a predetermined number of authentication cards 30 have been generated.

The selection engine 242 refers to a serial number generator 246, a dictionary database 248 and a random number generator 250 whilst making its selection. The serial number generator 246 generates sequential numbers of the form *nnnn - nnnn - nnnn - nnnn* (where *n* is a single digit integer) which are assigned as the serial numbers 40 of the authentication cards 30. The dictionary database 248 stores words 36 which have been chosen as being suitable for the purposes of the present invention. The suitability of a word is governed by many factors including, but not limited to, the type of word (nouns are better than adverbs), the number of letters comprising the word, the number of syllables in the word, how frequently the word is used in everyday language and the reading age associated with the word. Typically, the dictionary database 248 will store over 20,000 suitable words. The random number generator 250 is used for generating random numbers of a fixed digit length, four-digit numbers 38 are used in the previously described embodiments, and employs standard random number algorithms for this purpose.

A card generation process 260, which is performed by the authentication card generation system 240, is outlined in the flow diagram of Figure 14 and is discussed in more detail below.

When the selection engine 242 receives instructions from an authentication authority to generate a certain number of authentication cards 30, it commences the card generation process 260 at step 262 by calling the serial number generator 246 to determine a serial number 40 for a new authentication card 30.

The selection engine 242 then determines the 'word' and 'number' data sets, 32 and 34 respectively, which will be assigned to the serial number 40. At step 264, the selection engine 242 randomly selects, avoiding duplication, twenty words 36 from the dictionary database 248, by using standard database query techniques. The selected words 36 are preferably ordered into alphabetical order, ready for printing onto the authentication card 30 as the 'word' data set 32, and it is also advantageous if words starting with different letters are chosen (both aiding human look up speed). Similarly, at step 266, the selection engine 242 selects twenty numbers 38 (each number being four-digits in length) with which to form the 'number' data set 34 which will correspond to the 'word' data set 32. The engine 242 does this by calling the random number generator 250, which generates the numbers from an effective set of 10,000 members.

The 'word' data set 32, the 'number' data set 34 and the serial number 40 are combined in a data file and written to a batch processing data file at step 268 of the card generation process 260. The above steps 262 to 268 are then repeated, with new data files for different authentication cards being added to the batch processing file at step 268 until, at step 270, a predetermined batch file size is reached. Step 272 of the card generation process 260 is then executed, whereby the batch file containing all of the generated authentication card details is transmitted to the authentication system 24 and to the printing system 244 of the card manufacturer. In this way, the card

manufacturer is able to produce authentication cards 30 in accordance with the details held on the authentication system's database 50. The card generation process 260 is then repeated until the number of authentication cards 30 requested by the authentication authority have been generated.

Having described particular preferred embodiments of the present invention, it is to be appreciated that the embodiments in question are exemplary only, and that variations and modifications, such as those that will occur to those possessed of the appropriate knowledge and skills, may be made without departure from the spirit and scope of the invention as set forth in the appended claims. For example, it is possible to use more than two data sets. The authentication data may be subdivided into groups, such that, for example, there are four groups of data displayed on a card which are referred to by their group identifiers A, B, C and D. Each group would still contain two data sets of different information types, between whose members there is a unique correspondence, but the uniqueness of that correspondence then need only be limited to that particular group.

Similarly, it is possible to provide a user with multiple correct answers to be given to a challenge. For example, two or more words could be associated with a single number on the authentication card, such that when any of those words is provided as a response to the number when received as a challenge, the user is authenticated.

The authentication cards can also be provided with start dates and expiry dates determining their period of use. These dates would be stored in conjunction with the card's serial number in the authentication system's database. This could be of particular benefit to users when the card is used in conjunction with a password system. By associating an authentication card with the user's login account in this way, the user may be issued with a new authentication card without them having to change their username or password. The authentication system could detect when a card was due to expire and trigger a new authentication card to be produced for the user concerned, updating its records at the relevant times.

Finally, when used in conjunction with a payment card, the present invention can reduce the opportunity for fraud. Prior to the present invention there has been the possibility of merchants using validly obtained payment card details to elicit further payments from acquirers, which have not been authorised by the cardholder. If the acquirer also becomes the authentication authority, or if the acquirer requires an authentication signal from an authentication authority prior to processing a payment transaction, all merchants, whether bogus or genuine, would be prevented from using payment card details for a given transaction without the express permission of the payment card holder.

Claims:

1. A personal authentication store, for use in authenticating the identity of a user by determining a response to an authorisation challenge, the authentication store comprising:

a unique identifier for identifying the authentication store and hence the identity of the user;

a first subset of a plurality of humanly readable elements; and

a second subset of a plurality of humanly readable elements, each subset having been selected from a group of elements from a larger corresponding set and each element of the first subset being visually related to a specific one of the plurality of elements in the second subset,

wherein the unique identifier is related to each element of the first subset and to each respective corresponding visually related element of the second subset by machine stored information external to the store such that authentication of the personal store requires the use of the machine stored information to verify the visual relationship between an element of the first subset provided as the authentication challenge and an element of the second subset provided as the response thereto.

2. A personal authentication store of Claim 1, wherein the visual relationship between the elements of the first and second subsets comprises a positional relationship, a colour relationship or a graphical relationship in the personal store.

3. A personal authentication store of Claim 1 or 2, wherein the elements of one of the first or the second subsets comprise features of the visual relationship.

4. A personal authentication store of Claim 1 or 2, wherein the elements of the first and second subsets comprise alphanumeric characters.

5. A personal authentication store of Claim 4, wherein the alphanumeric characters have a minimum font size of ten points.

6. A personal authentication store of Claim 4, wherein one of the first and second subsets comprises words.

7. A personal authentication store of Claim 6, wherein one of the first and second subsets comprises words selected from a list of words suitable to minimise errors when verbally spoken across a telecommunications network.

8. A personal authentication store of Claim 7, wherein one of the first and second subsets comprises nouns.

9. A personal authentication store of Claim 7 or 8, wherein one of the first and second subsets comprises words with one or two syllables.

10. A personal authentication store of any of Claims 7 to 9, wherein one of the first and second subsets comprises words from a predetermined set of commonly spoken words.

11. A personal authentication store of any of Claims 7 to 10, wherein one of the first and second subsets comprises simple words commensurate with a reading age of eight years.

12. A personal authentication store of any of Claims 7 to 11, wherein one of the first and second subsets comprise words with a maximum length of eight letters.

13. A personal authentication store of any of Claims 4 to 12, wherein one of the first and the second subsets comprises a set of numbers.

14. A personal authentication store of Claim 13, wherein each of the elements of the first or second subsets comprises a four digit to six digit number.

15. A personal authentication store of any of Claims 4 to 14, wherein the alphanumeric character elements of one of the first or second subsets is arranged in alphabetic or numeric order.

16. A personal authentication store of any preceding claim, wherein the first subset comprises a different type of information to that of the second subset.

17. A personal authentication store of any preceding claim, wherein the first subset and the second subset comprise data which is not personal to the user.

18. A personal authentication store of any preceding claim, wherein each element of first subset has only a single unique corresponding element in the second subset.

19. A personal authentication store of any preceding claim, wherein each element of the second subset comprises a plurality of items, any of the items being validly providable as the response to the corresponding authentication challenge.

20. A personal authentication store of any preceding claim, wherein the first and/or second subset comprises a plurality of randomly selected data elements.

21. A personal authentication store of any preceding claim, wherein the authentication store comprises an electronic device in which the first and second subsets can be held and displayed.

22. A personal authentication store of Claim 21, wherein the electronic device comprises a mobile telephone, a personal digital assistant or other mobile computing device.

23. A personal authentication store of any of Claims 1 to 20, wherein the authentication store comprises a portable card.

24. A personal authentication store of Claim 23, wherein the card comprises means for preventing the first and second subsets of elements from being readable when the same are photocopied.

25. A personal authentication store of Claim 24, wherein the preventing means comprises a coating, ink or film which diffuses, diffracts or scatters light.

26. A personal authentication store of any of Claims 23 to 25, wherein the authentication store comprises covering means for rendering the first and second subsets initially unreadable, the covering means being operable in an irreversible manner to render the first and second subsets readable.

27. A personal authentication store of Claim 26, wherein the covering means comprises a tamper-evident envelope within which the authentication store is initially provided.

28. A personal authentication store of Claim 26 or 27, wherein the covering means comprises a scratch-off coating.

29. A personal authentication store of any preceding claim, further comprising information defining a financial transaction card, for example a credit card.

30. A personal authentication store of Claim 29, wherein the unique identifier comprises a PAN (Primary Account Number) of a credit, debit or charge card.

31. A personal authentication store of Claim 30, wherein the first subset of elements and the second subset of elements are provided on one face of the authentication store and the unique identifier and the information defining the financial transaction card is provided on another face of the authentication store.

32. A personal authentication store of Claim 29, 30 or 31, further comprising an electronic memory or a magnetic strip for storing the financial transaction card information.

33. A personal authentication store of any preceding claim, wherein the authentication store has a prepayment value associated with it and means for identifying the prepayment value to the user.

34. A personal authentication store of any preceding claim, wherein the unique identifier comprises a serial number.

35. A personal authentication store of any preceding claim, wherein the unique identifier comprises a machine readable number or number representation, such as a bar code.

36. A method of authenticating a personal authentication store for use in authenticating the identity of a user, the method comprising:

receiving a unique identifier of the personal authentication store;

identifying first and second subsets of predetermined data elements using the unique identifier, each subset having been previously selected from a corresponding larger set of the data elements and each data element of the first subset corresponding to a specific one of the data elements of the second subset;

selecting a data element from the first subset and transmitting the data element to the user as an authentication challenge;

receiving a response to the authentication challenge from the user that has been determined by use of information provided on the personal authorisation store; and

issuing an authentication signal if the response comprises the specific data element of the second subset that corresponds to the data element of the first subset used for the challenge.

37. A method of Claim 36, wherein the receiving step comprises receiving a response to the authentication challenge from the user that has been determined by use of information provided on a personal authorisation store according to any of Claims 1 to 35.

38. A method of Claim 36 or 37, wherein the transmitting and receiving steps comprise transmitting and receiving information over a telecommunications link such that remote authorisation of a user can be carried out.

39. A method of Claim 38, wherein the transmitting and receiving steps comprise transmitting and receiving information via the Internet or a short messaging service (SMS) exchange.

40. A method of any of Claims 36 to 39, wherein the selection step comprises selecting an element of the first data subset at random.

41. A method of Claim 40, wherein the selection step comprises selecting an element of the first data subset randomly on first use of the personal authentication store and thereafter selecting an element of the first data subset deterministically such that a previously selected element has a lower chance of being selected than a previously not selected element.

42. A method of any of Claims 36 to 39, wherein the selection step comprises selecting an element of the first data subset sequentially in the order that the elements are displayed on the user's personal authentication store.

43. A method of any of Claims 36 to 42, wherein the transmitting step comprises transmitting a random data element together with the authentication challenge and the receiving step comprises receiving the random data element from the user encrypted with the response to the challenge as a key,

the method further comprising using the specific data element of the second subset that corresponds to the data element of the first subset used for the challenge to decrypt the received data, and

carrying out the issuing step only if the decrypted data is equivalent to the random data element transmitted to the user.

44. A method of any of Claims 36 to 43, wherein the receiving step comprises receiving representations of the information provided on the authentication store as the response.

45. A method of Claim 44, wherein the representations represent positional co-ordinates, such as those provided by a mouse click, and the method further comprises converting the representations into the information provided on the authentication card.

46. A method of any of Claims 36 to 45, further comprising selecting which of two selected data sets is to act as the first data set and which is to act as the second data set.

47. A method of any of Claims 36 to 46, further comprising

transmitting a request for a Personal Identification Number (PIN) associated with the authentication store;

receiving a number from the user in response to the request; and

comparing the received number with a pre-stored PIN for the authentication store.

48. A method of any of Claims 36 to 47, further comprising making services available to the user in response to issuance of the authentication signal.

49. A method of Claim 48, wherein the making further services available step comprises making prepaid services available to the user.

50. A method of Claim 49, wherein the method further comprises reducing a prepayment value stored in a prepayment field in accordance with the use of the prepaid services.

51. A method of any of Claims 36 to 50, further comprising processing a payment transaction in response to the issuance of the authentication signal.

52. A method of any of Claims 36 to 51, wherein the step of receiving the unique identifier comprises:

issuing a login and password challenge to the user;

receiving a login identifier and a password response;

part-verifying the identity of the user if the password matches the pre-stored password associated with that login identifier for that user; and

retrieving the unique identifier associated with the personal store issued to that user.

53. A system for authenticating a personal authentication store for use in authenticating the identity of a user, the system comprising:

a receiving means for receiving a unique identifier of the personal authentication store;

identifying means for identifying first and second subsets of predetermined data elements using the unique identifier, each subset having been previously selected from a corresponding larger set of the data elements and each data element of the first subset corresponding to a specific one of the data elements of the second subset;

selecting means for selecting a data element from the first subset;

transmitting means for transmitting the data element to the user as an authentication challenge;

the receiving means being arranged to receive a response to the authentication challenge from the user that has been determined by use of information provided on the personal authorisation store; and

issuing means for issuing an authentication signal if the response comprises the specific data element of the second subset that corresponds to the data element of the first subset used for the challenge.

54. A combination of a personal authentication store as claimed in any of Claims 1 to 35 and a system as claimed in Claim 53.

55. A method of configuring a personal authentication store, for use in authenticating the identity of a user by determining a response to an authorisation challenge, the method comprising:

determining a unique identifier for identifying the authentication store;

selecting a first subset of a plurality of humanly readable elements from a corresponding larger set of the elements;

selecting a second subset of a plurality of humanly readable elements from a corresponding larger set of the elements;

relating the unique identifier to the first and second selected subsets and relating elements within the first subset to corresponding elements within the second subset, such that the elements of the first and second subsets can be used to validate the authenticity of the personal authentication store; and

storing the unique identifier, the first subset and the second subset in the personal identification store, such that each element of the first subset is visually related to a specific one of the plurality of elements in the second subset, thereby enabling the user to determine which element of the second subset is to form a response to a challenge comprising an element of the first subset.

56. A method of Claim 55, wherein either of the selecting steps comprises selecting the plurality of humanly readable elements which make up the subset randomly from the corresponding larger set of elements.

57. A method of Claim 55, wherein either of the selecting steps comprises selecting the plurality of humanly readable elements which make up the subset deterministically such that there is no duplication of elements in any of the subsets.

58. A method of any of Claims 55 to 57, wherein the humanly readable elements of one of the first and second subsets comprises words and the method further comprises creating the corresponding larger set of the elements as a list of words which are suitable for minimising errors when verbally spoken across a telecommunications network.

59. A method of any of Claims 55 to 58, wherein the humanly readable elements of one of the first and second subsets comprises words and the method further comprises creating the corresponding larger set of the elements as a list of commonly spoken words.

60. A method of Claim 58 or 59, wherein the creating step comprises removing words from the list of words which require a higher reading age than eight, which have an ability to be easily misread by a dyslexic user, which have more than two syllables or which are longer than eight letters in length.

61. A method of any of Claims 55 to 60, wherein the relating step comprises relating each element within the first subset to only a single unique corresponding element within the second subset.

62. A method of any of Claims 55 to 61, wherein the elements of the first or second subsets comprise alphanumeric characters and the storing step comprises arranging the elements of the first or second subset in alphabetic or numeric order in the personal authentication store.

63. A method of any of Claims 55 to 62, wherein the storing step comprises transmitting data representing the unique identifier, the first data subset and the second data subset to the personal authentication store and the method further comprises activating the personal authentication store to display the transmitted data.

64. A system for configuring a personal authentication store, for use in authenticating the identity of a user by determining a response to an authorisation challenge, the system comprising:

determining means for determining a unique identifier for identifying the authentication store;

first selecting means for selecting a first subset of a plurality of humanly readable elements from a corresponding larger set of the elements;

second selecting means for selecting a second subset of a plurality of humanly readable elements from a corresponding larger set of the elements;

relating means arranged to relate the unique identifier to the first and second selected subsets and relating elements within the first subset to corresponding elements within the second subset, such that the elements of the first and second subsets can be used to validate the authenticity of the personal authentication store; and

storing means arranged to store the unique identifier, the first subset and the second subset in the personal identification store, such that each element of the first subset is visually related to a specific one of the plurality of elements in the second subset, thereby enabling the user to determine which element of the second subset is to form a response to a challenge comprising an element of the first subset.

65. A combination of a personal authentication store as claimed in any of Claims 1 to 35 and a system as claimed in Claim 64.

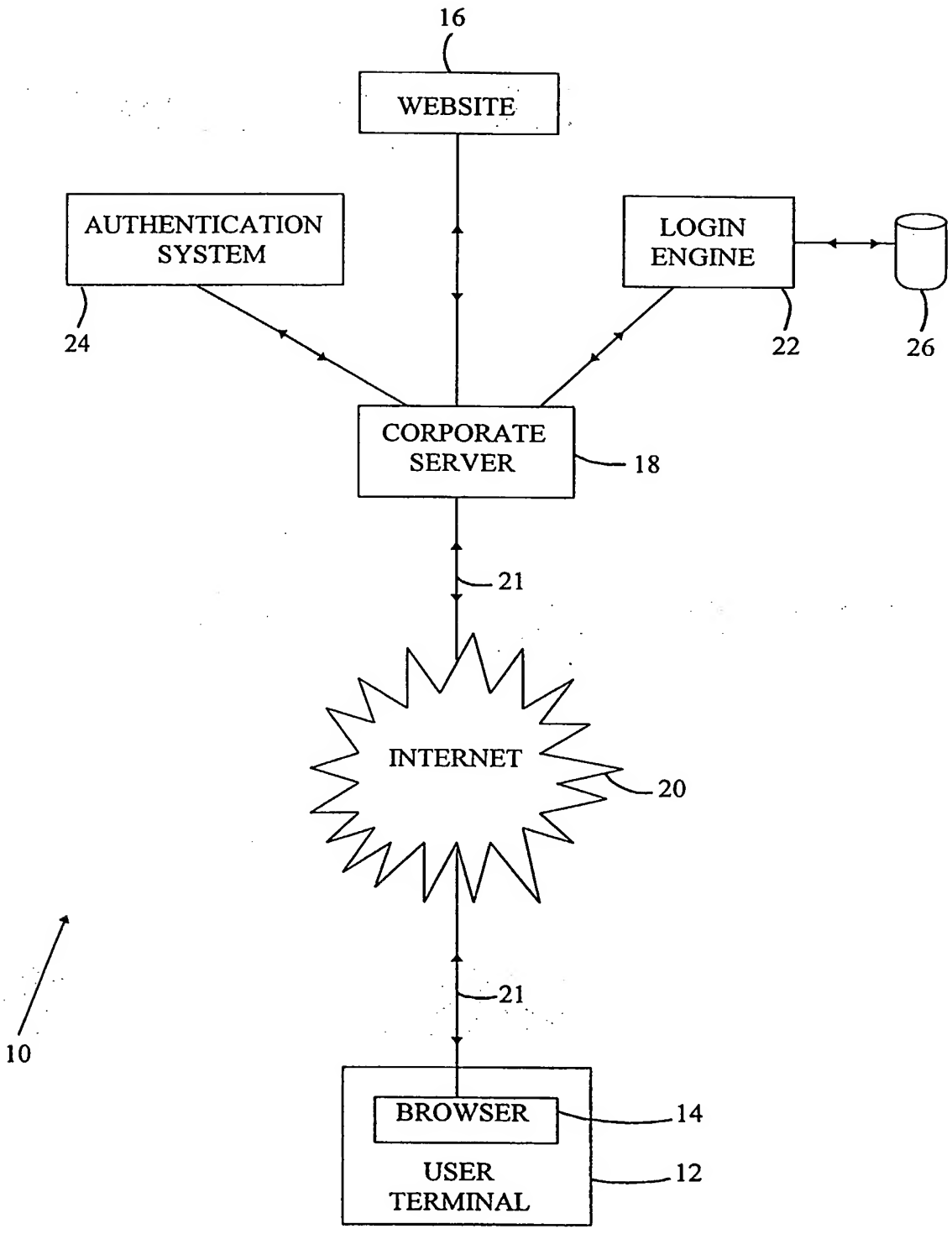

16
WEBSITE
AUTHENTICATION SYSTEM
LOGIN ENGINE
24
22
26
CORPORATE SERVER
18
21
INTERNET
20
21
10
BROWSER
14
USER TERMINAL
12

Figure 1

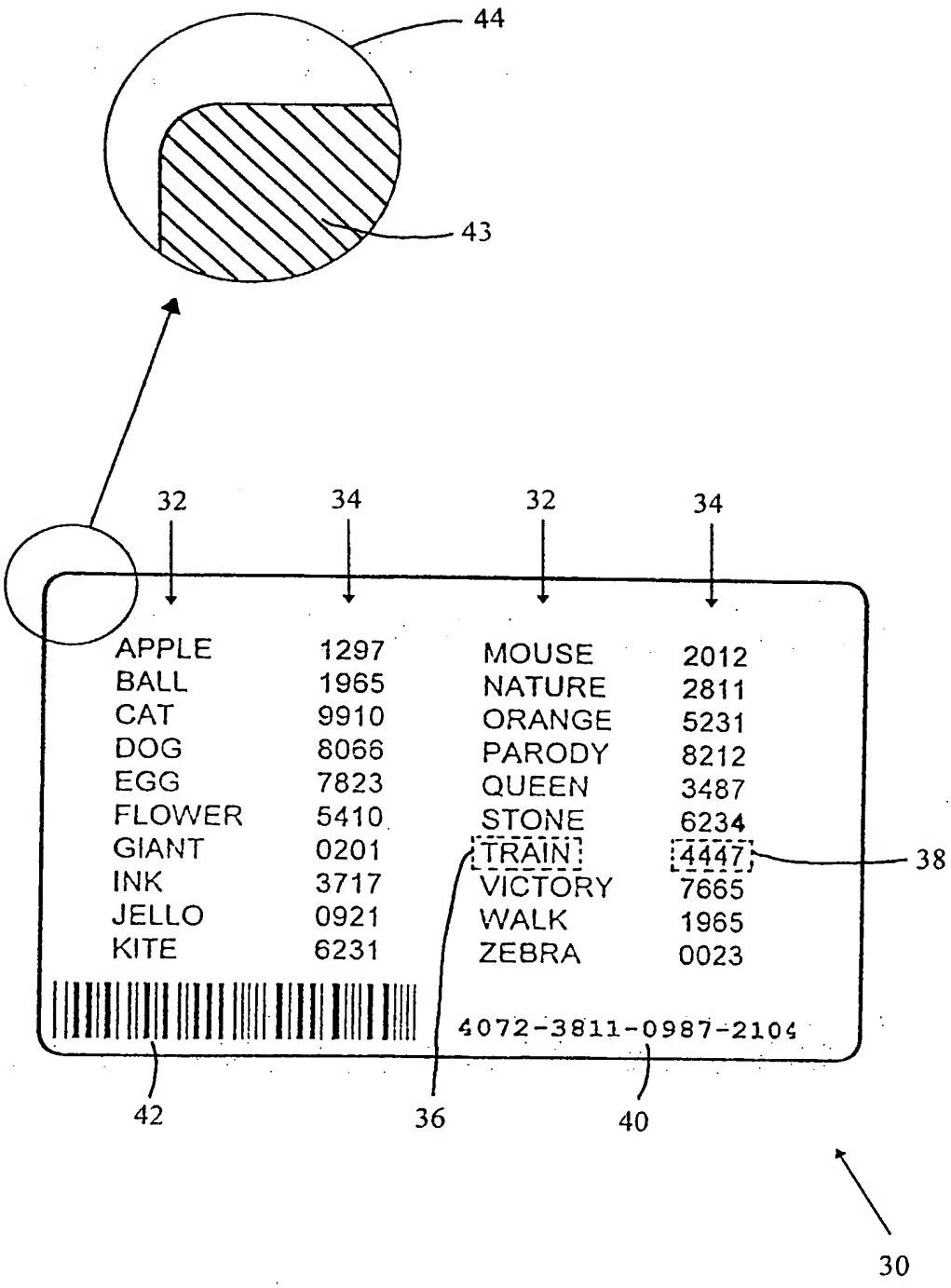

44
43
32
34
32
34
APPLE 1297
BALL 1965
CAT 9910
DOG 8066
EGG 7823
FLOWER 5410
GIANT 0201
INK 3717
JELLO 0921
KITE 6231
MOUSE 2012
NATURE 2811
ORANGE 5231
PARODY 8212
QUEEN 3487
STONE 6234
TRAIN 4447
VICTORY 7665
WALK 1965
ZEBRA 0023
4072-3811-0987-2104
38
42
36
40
30

Figure 2

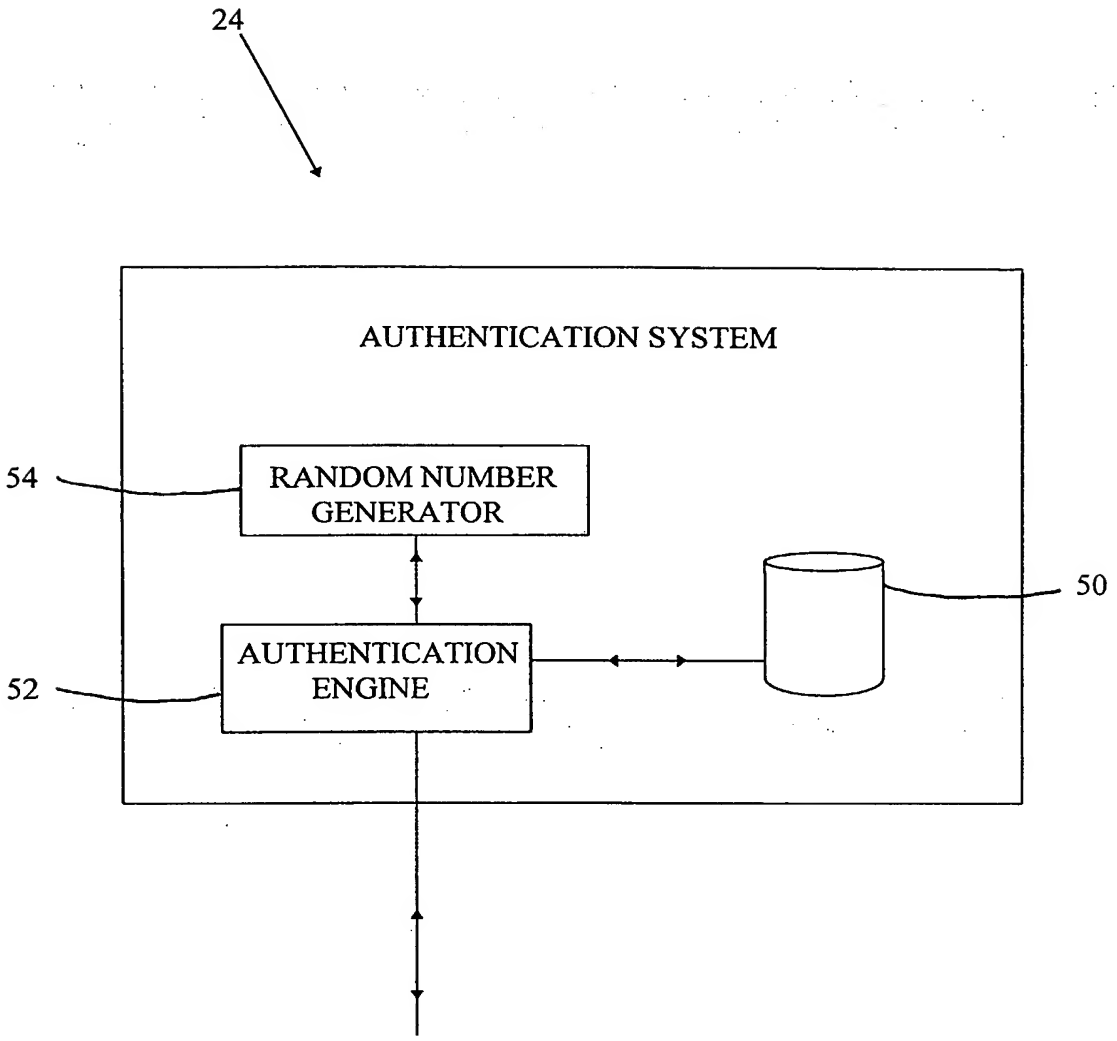

24
AUTHENTICATION SYSTEM
54
RANDOM NUMBER GENERATOR
50
AUTHENTICATION ENGINE
52

Figure 3

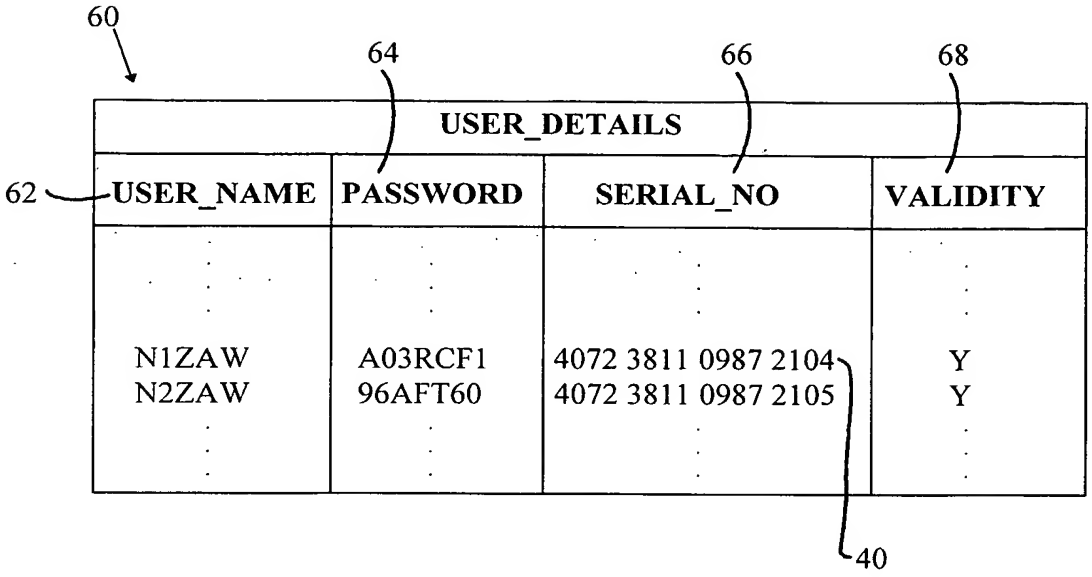


Figure 4

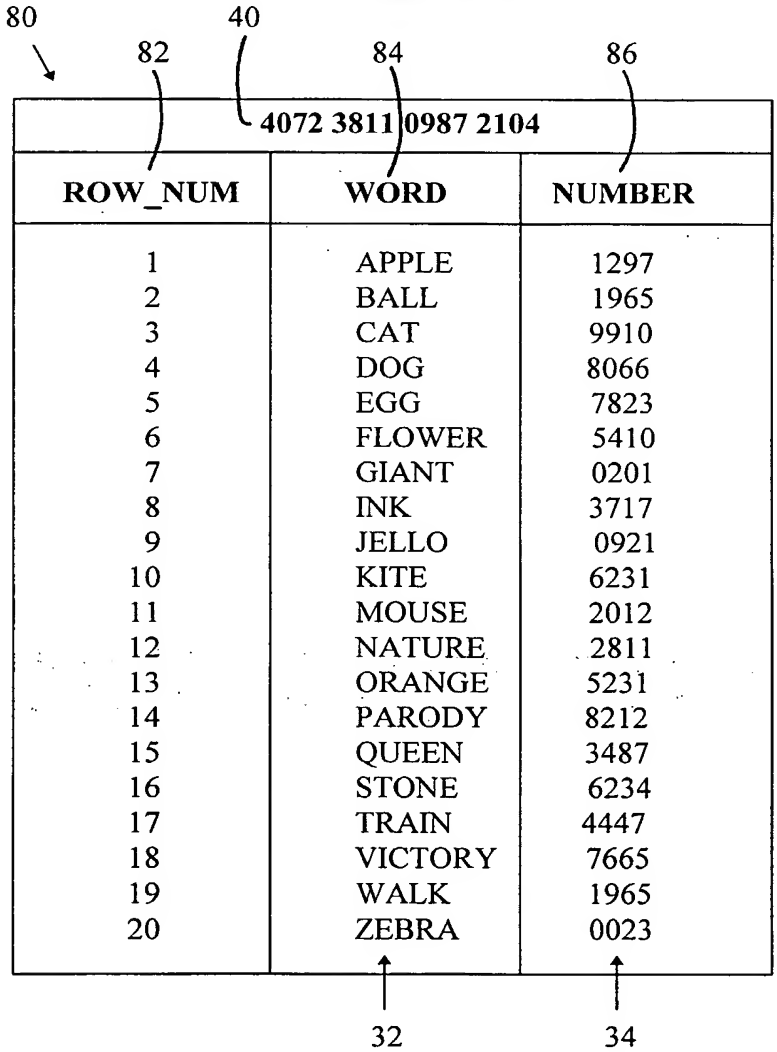


Figure 5

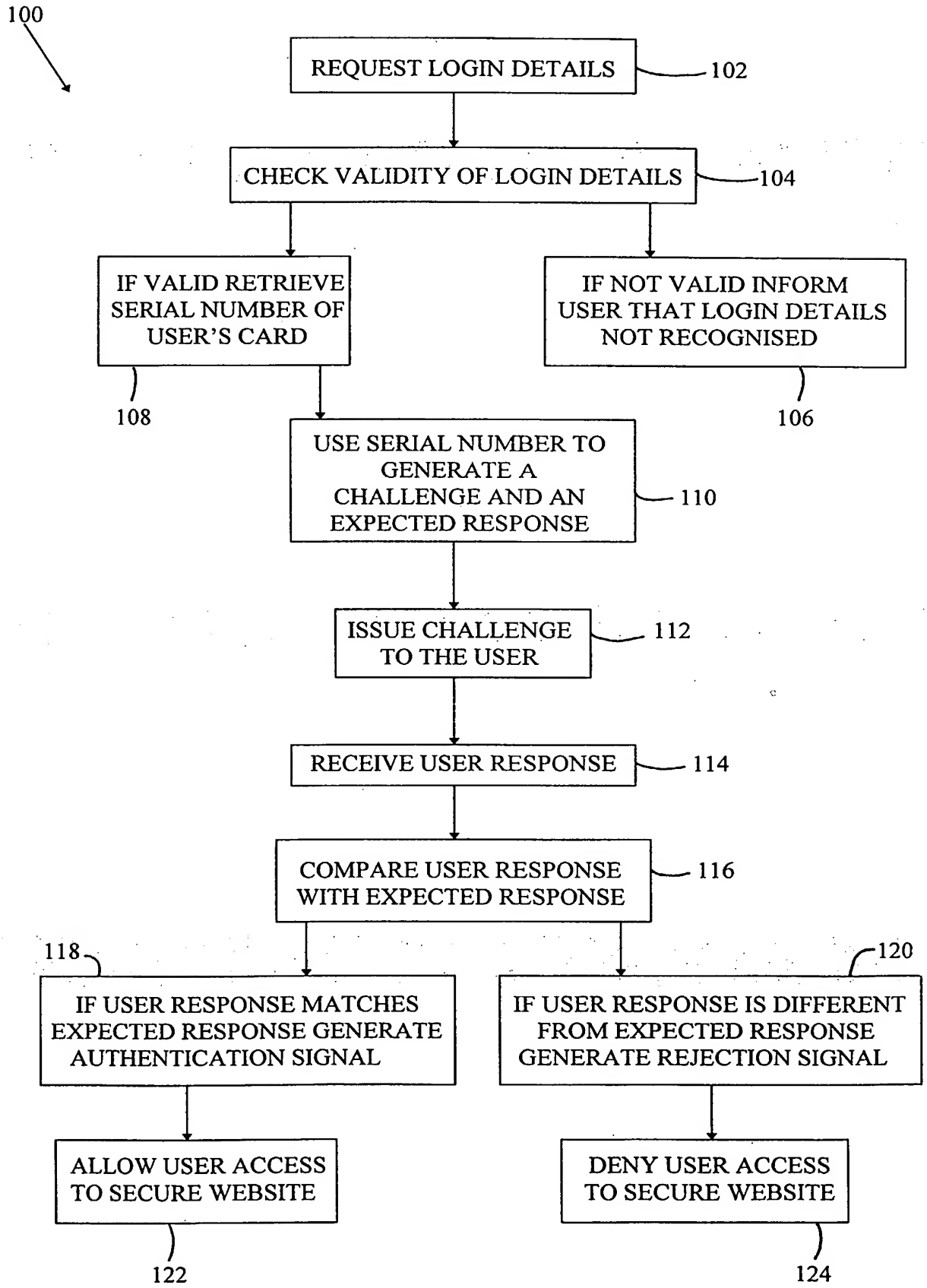

100
REQUEST LOGIN DETAILS
102
CHECK VALIDITY OF LOGIN DETAILS
104
IF VALID RETRIEVE SERIAL NUMBER OF USER'S CARD
IF NOT VALID INFORM USER THAT LOGIN DETAILS NOT RECOGNISED
108
106
USE SERIAL NUMBER TO GENERATE A CHALLENGE AND AN EXPECTED RESPONSE
110
ISSUE CHALLENGE TO THE USER
112
RECEIVE USER RESPONSE
114
COMPARE USER RESPONSE WITH EXPECTED RESPONSE
116
118
120
IF USER RESPONSE MATCHES EXPECTED RESPONSE GENERATE AUTHENTICATION SIGNAL
IF USER RESPONSE IS DIFFERENT FROM EXPECTED RESPONSE GENERATE REJECTION SIGNAL
ALLOW USER ACCESS TO SECURE WEBSITE
DENY USER ACCESS TO SECURE WEBSITE
122
124

Figure 6

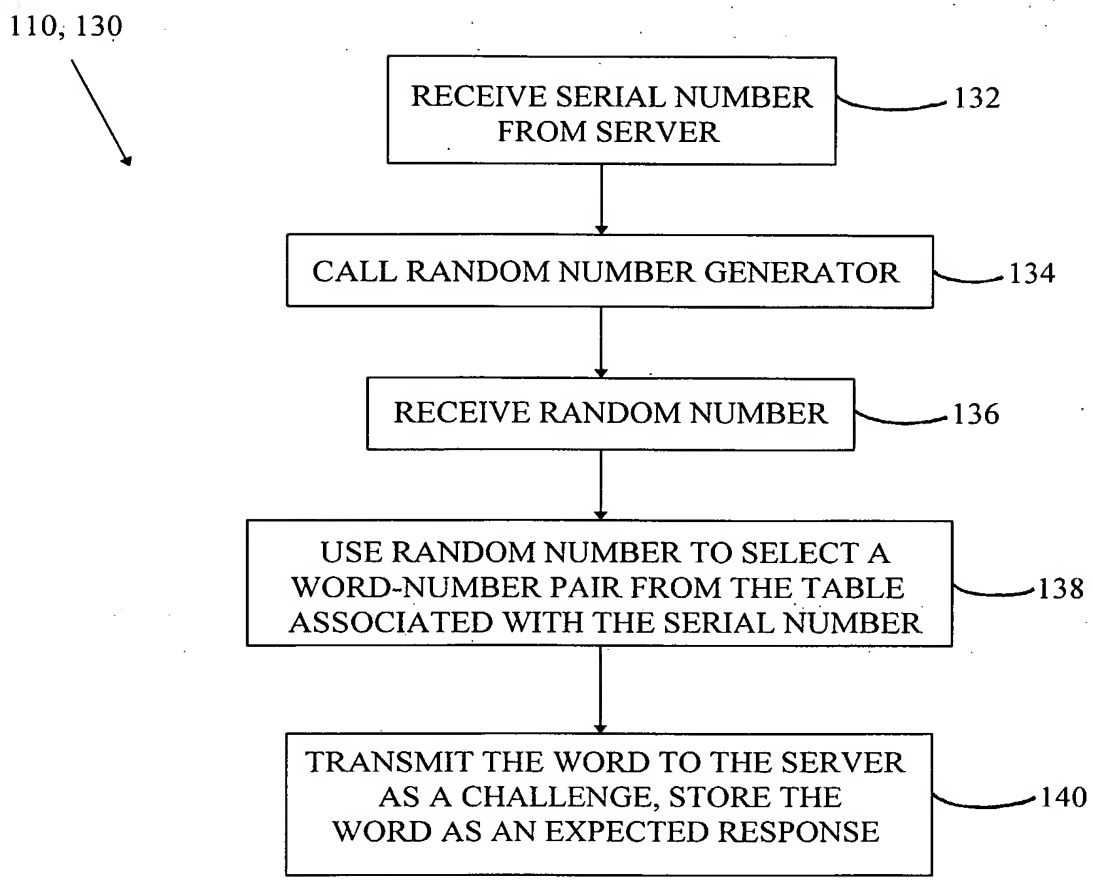

110, 130
RECEIVE SERIAL NUMBER FROM SERVER
132
CALL RANDOM NUMBER GENERATOR
134
RECEIVE RANDOM NUMBER
136
USE RANDOM NUMBER TO SELECT A WORD-NUMBER PAIR FROM THE TABLE ASSOCIATED WITH THE SERIAL NUMBER
138
TRANSMIT THE WORD TO THE SERVER AS A CHALLENGE, STORE THE WORD AS AN EXPECTED RESPONSE
140

Figure 7

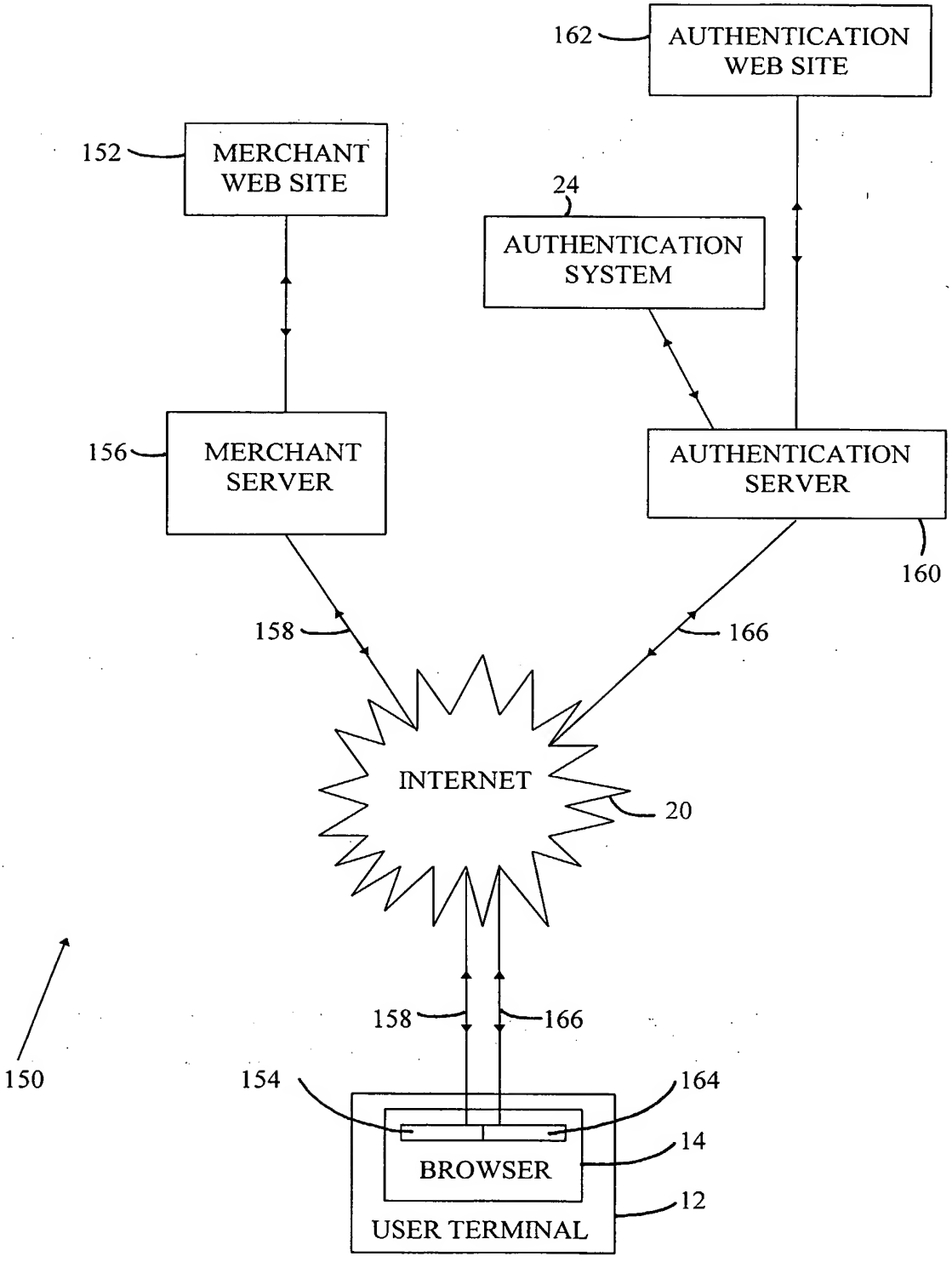

162
AUTHENTICATION WEB SITE
152
MERCHANT WEB SITE
24
AUTHENTICATION SYSTEM
156
MERCHANT SERVER
AUTHENTICATION SERVER
160
158
166
INTERNET
20
150
158
166
154
164
14
BROWSER
12
USER TERMINAL

Figure 8

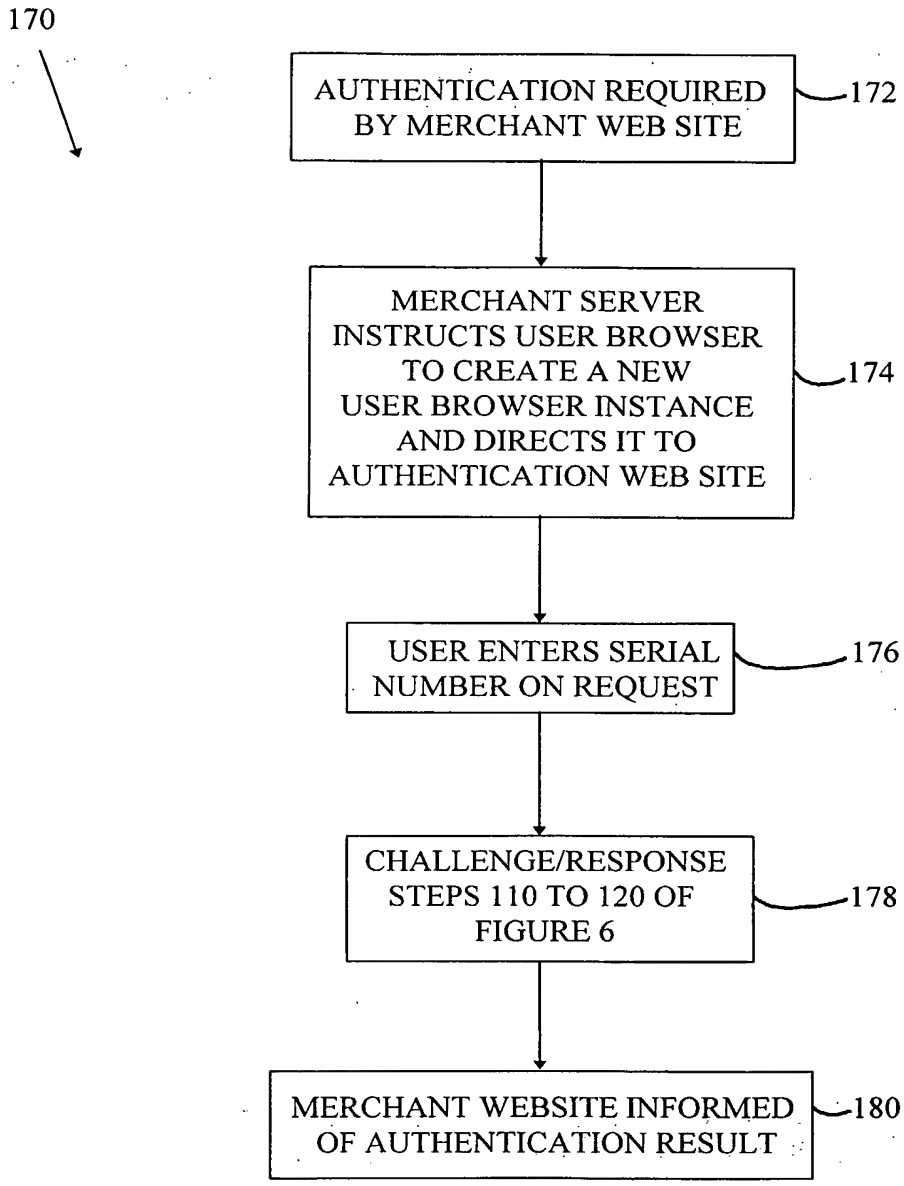

170
AUTHENTICATION REQUIRED BY MERCHANT WEB SITE
172
MERCHANT SERVER INSTRUCTS USER BROWSER TO CREATE A NEW USER BROWSER INSTANCE AND DIRECTS IT TO AUTHENTICATION WEB SITE
174
USER ENTERS SERIAL NUMBER ON REQUEST
176
CHALLENGE/RESPONSE STEPS 110 TO 120 OF FIGURE 6
178
MERCHANT WEBSITE INFORMED OF AUTHENTICATION RESULT
180

Figure 9

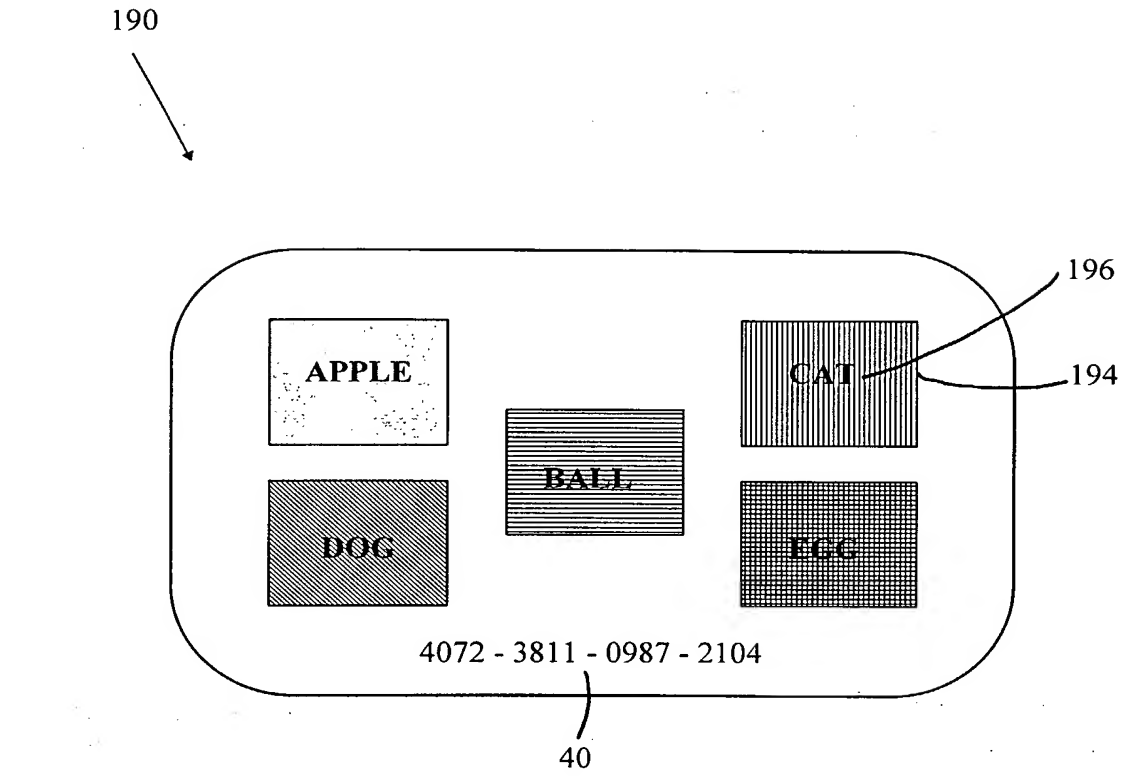

190
196
194
APPLE
BALL
CAT
DOG
EGG
4072 - 3811 - 0987 - 2104
40
192
SHADING KEY:
BLUE
YELLOW
PURPLE
ORANGE
PINK

Figure 10

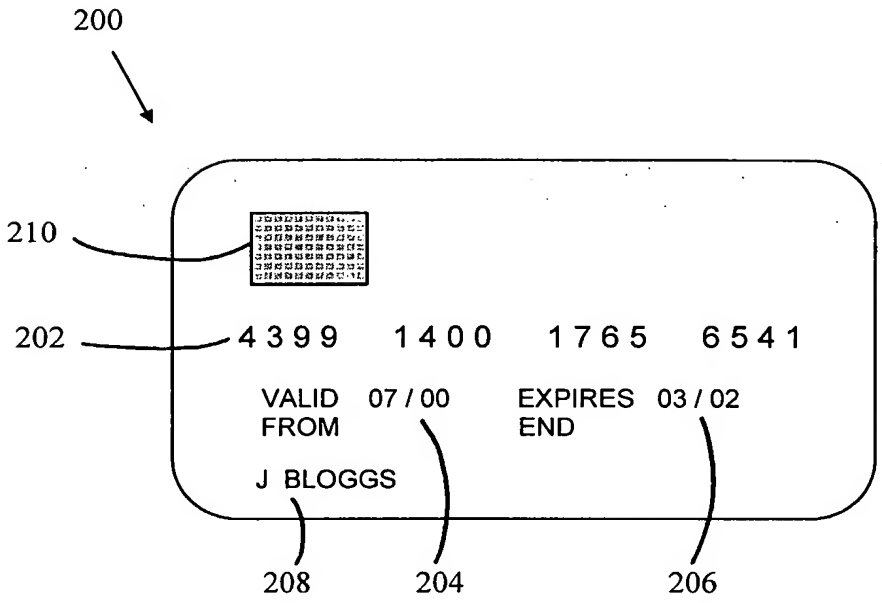


Figure 11a

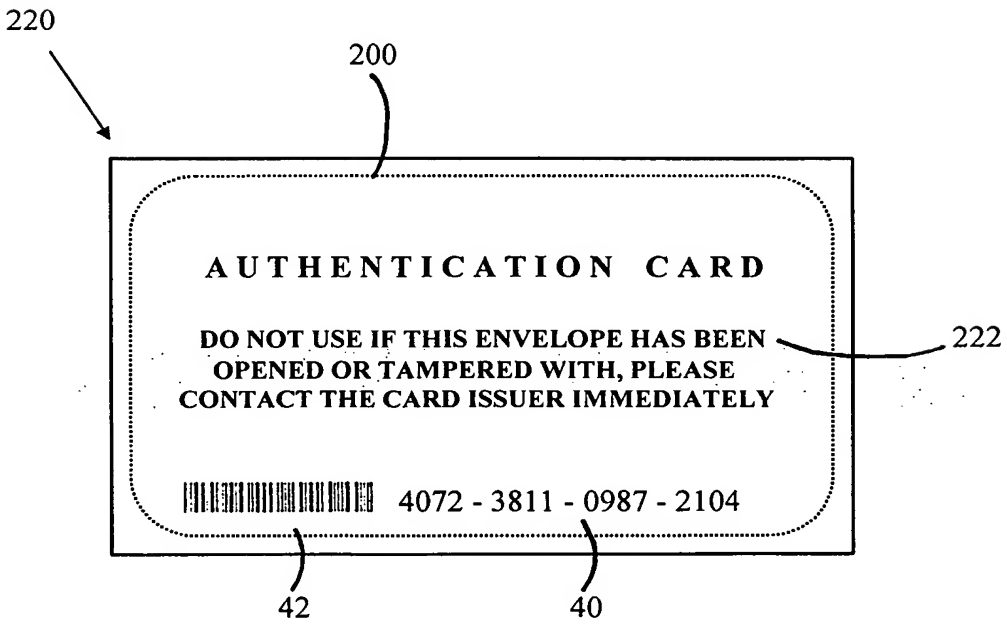


Figure 11b

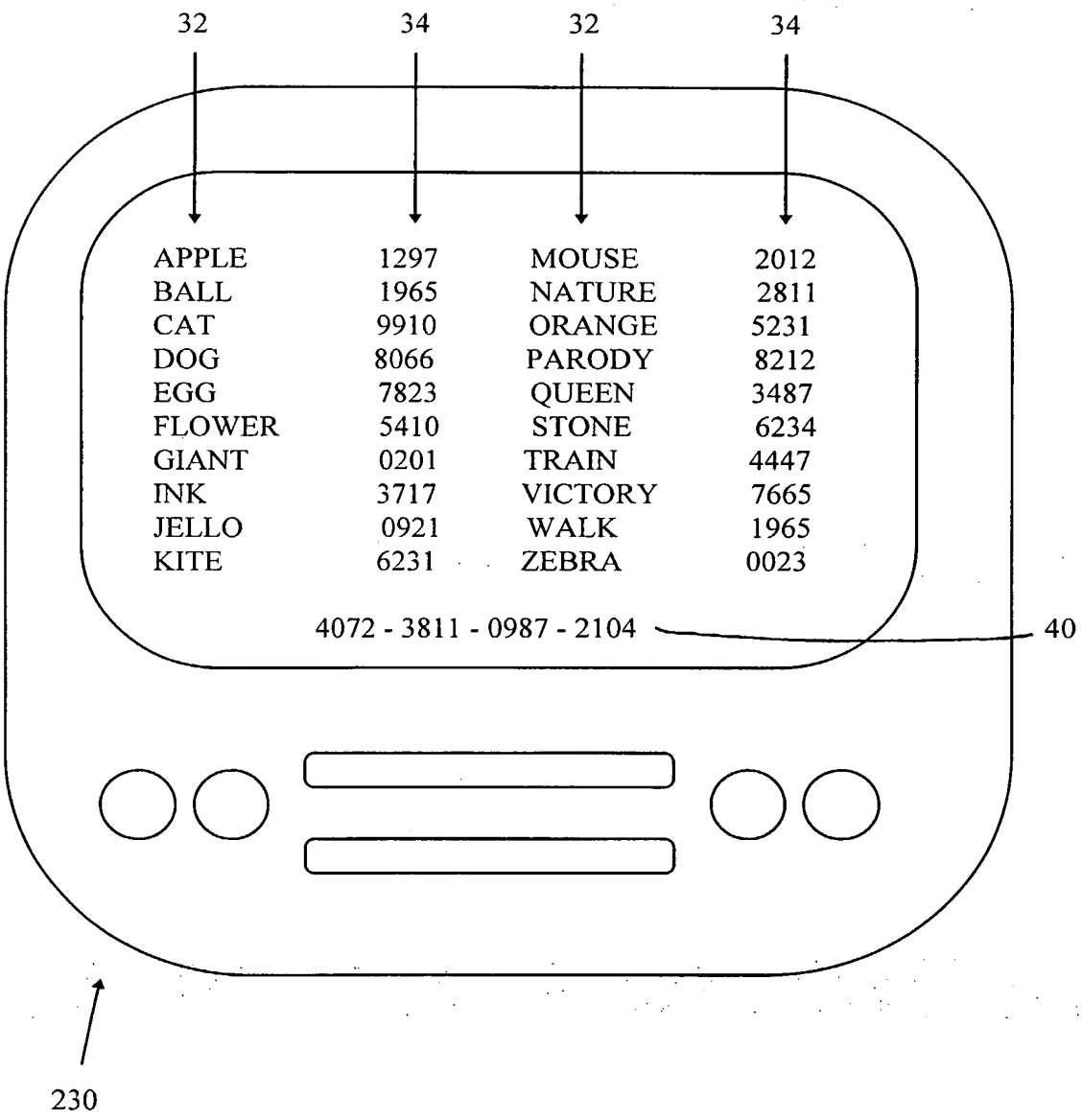

32
34
32
34
APPLE 1297 MOUSE 2012
BALL 1965 NATURE 2811
CAT 9910 ORANGE 5231
DOG 8066 PARODY 8212
EGG 7823 QUEEN 3487
FLOWER 5410 STONE 6234
GIANT 0201 TRAIN 4447
INK 3717 VICTORY 7665
JELLO 0921 WALK 1965
KITE 6231 ZEBRA 0023
4072 - 3811 - 0987 - 2104
40
230

Figure 12

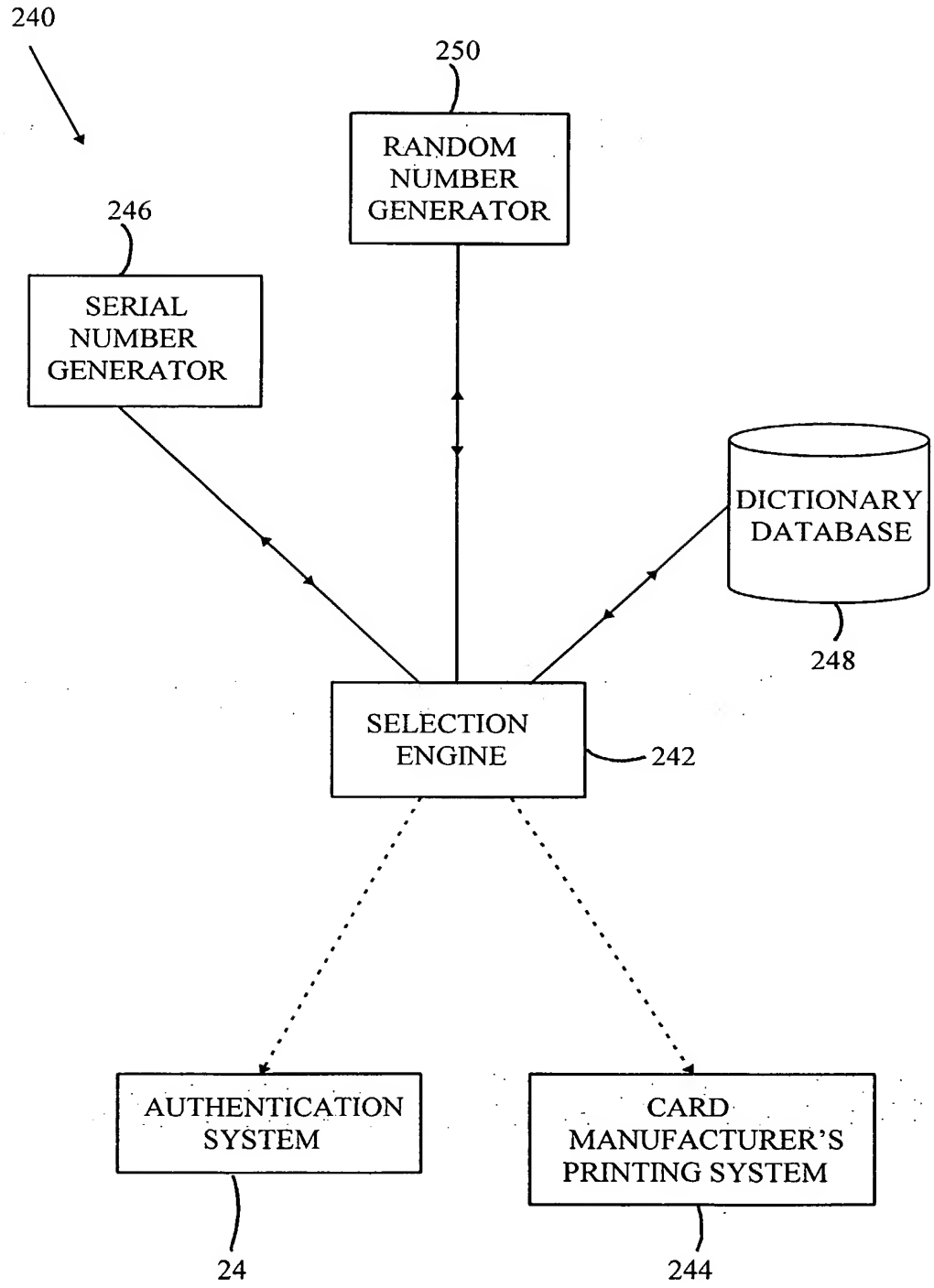

240
250
RANDOM NUMBER GENERATOR
246
SERIAL NUMBER GENERATOR
DICTIONARY DATABASE
248
SELECTION ENGINE
242
AUTHENTICATION SYSTEM
24
CARD MANUFACTURER'S PRINTING SYSTEM
244

Figure 13

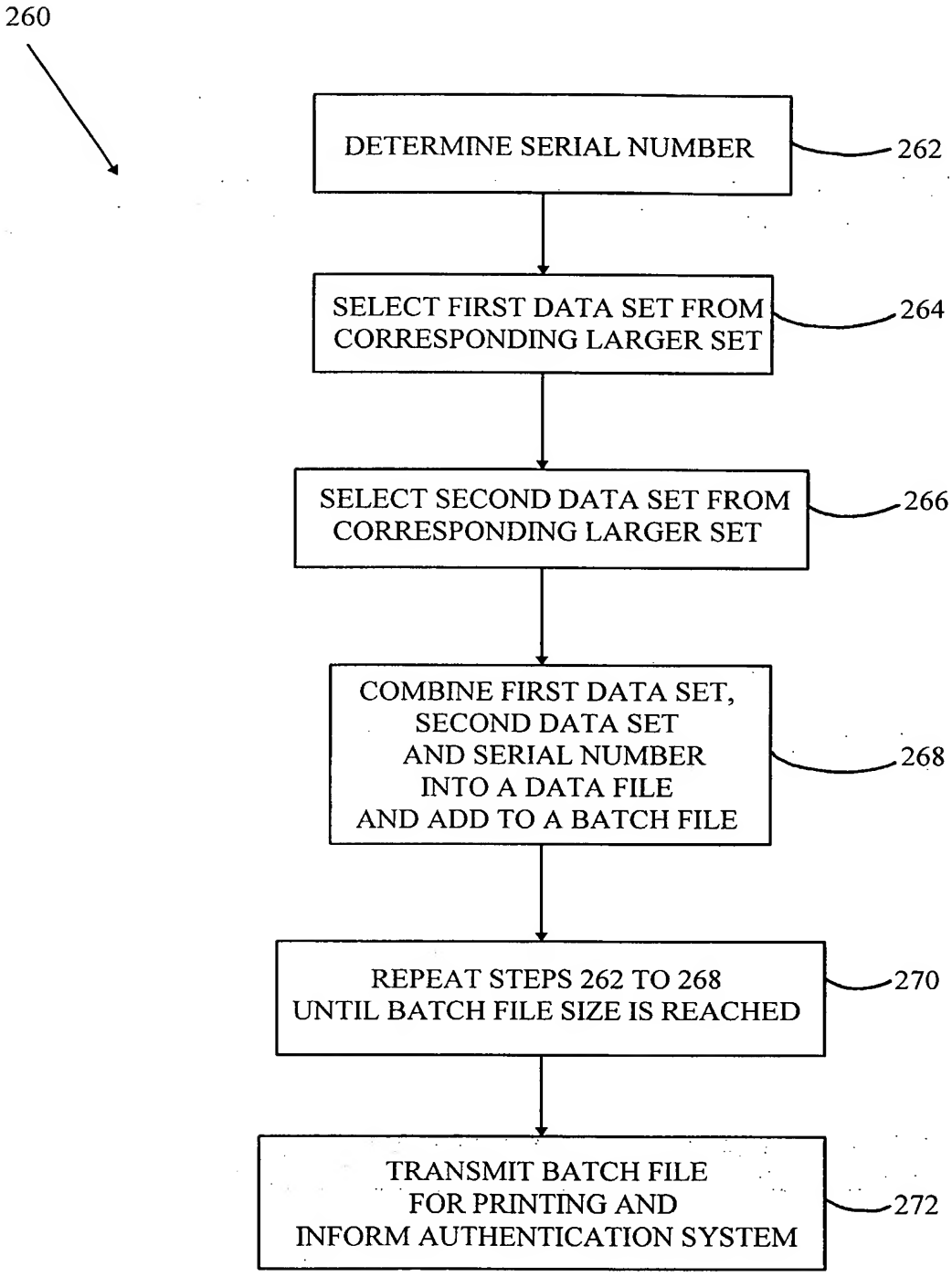

260
DETERMINE SERIAL NUMBER
262
SELECT FIRST DATA SET FROM CORRESPONDING LARGER SET
264
SELECT SECOND DATA SET FROM CORRESPONDING LARGER SET
266
COMBINE FIRST DATA SET, SECOND DATA SET AND SERIAL NUMBER INTO A DATA FILE AND ADD TO A BATCH FILE
268
REPEAT STEPS 262 TO 268 UNTIL BATCH FILE SIZE IS REACHED
270
TRANSMIT BATCH FILE FOR PRINTING AND INFORM AUTHENTICATION SYSTEM
272

Figure 14